ON RADICAL MODULES AND SPACES

Inaugural-Dissertation
zur
Erlangung der Doktorwürde
des Fachbereichs Mathematik
der Freien Universität Berlin

vorgelegt von
Günter Wicke
aus Plauen im Vogtland

Berlin 1974

1975

ON RADICAL MODULES AND SPACES

Inaugural-Dissertation
zur
Erlangung der Doktorwürde
des Fachbereichs Mathematik
der Freien Universität Berlin

vorgelegt von
Günter Wicke
aus Plauen im Vogtland

Berlin 1974

1. Referent: Prof. Dr. A. Fröhlich, London

2. Referent: Prof. Dr. U. Güntzer, Berlin

UNIV.
LEIDEN
BIBL.

Tag der mündlichen Prüfung: 27. Februar 1975

Druck: Der Präsident der Freien Universität Berlin – Zentrale Universitätsdruckerei V aA 4, 1 Berlin 41

T A B L E O F C O N T E N T S

Introduction and Preview of Results 4

I Preliminaries on Radical Spaces and Radical Modules

1. Notation and Definitions 8

2. An Elementary Characterization and some Fundamental Properties of Radical Modules and Spaces 10

3. Group Theoretic Characterization of Radicals, Radical Spaces, and Modules 17

4. Summary on Valuations of Radicals, Radical Spaces, and Radical Modules 21

II Number-Theoretic Investigations on Radicals and Radical Modules

5. Integral and Unit Elements, a Norm for Radical Modules 23

6. Examples from Multiplicative Number Theory for Radical Modules 28

7. Extension of a Theorem of Minkowski's to Radical Modules 33

8. Integral Radical Modules of a Radical Subspace 35

III Radicals over Local Fields

9. The Valuation Maps v, v^*, $\hat{v}$ 39

10. On the Structure of $R(K)$ for Locally Complete K 43

IV Applications to Global and $\mathfrak{p}$-adic Number Fields

11. Global Maps Induced by Valuations and the Ideal Class Group 50

12. An Estimate for Element-Resolvents over a $\mathfrak{p}$-adic Number Field 60

Literature 68

Introduction and Preview of Results

Both, radical spaces and radical modules, are notions first introduced by A. Fröhlich in 1966 in a paper published in honour of T. Nakayama (cf [1]).

A radical space is a one dimensional vectorspace over a field K generated by a radical of K, i.e. by an element of an algebraic closure $\overline{K}$ of K a power of which lies in K.

In the case that K is a quotient field of a Dedekind domain o radical modules form, generally speaking, a subgroup of the finitely generated projective o-modules contained in $\overline{K}$.

Apart from this view of radical modules chapter I of this paper provides two more characterizations. Fröhlich's original approach is outlined in section 1 defining radical spaces first and then radical modules as finitely generated submodules of radical spaces. - Another more elementary way is to operate with fractional ideals of the underlying field. A radical module then is the product of a fractional ideal and a radical. This is carried through in section 2.

Chapter II exploits the fact that the group $\mathfrak{R}(o)$ of radical modules contains as a subgroup the fractional ideals of K/o. It is shown that some number theoretic notions, among them the absolute norm, can be defined in an appropriate way such that a number of theorems on fractional ideals carry over to radical modules. A typical example provides section 7 where

Minkowski's theorem on the existence in every ideal class of an integral ideal whose norm lies below a fixed determined bound is extended to radical modules.

Throughout chapter II valuation theory of radical modules has been used as a tool of definition. I would like to point out here that this has been done purely for reasons of convenience. All considerations of chapter II could have been conducted globally, the definition of norm included. At various instances the equivalent global versions are given.

For the considerations of chapter III and IV, however, valuation theory cannot be abandoned. Section 9 is of a preparatory nature and provides information on the kernels and cokernels of the valuation maps involved.

In section 10 the case of locally complete base field and its radicals is taken up. The factor groups of radicals modulo the unit radicals are determined as well as that of the unit radicals modulo all roots of unity.

The local maps of section 9 are put together in section 11 to obtain global statements involving the ideal class group. The torsion part of the ideal class group in the general case can be described as factor group of unit radical modules by the principal ones, which, for algebraic number fields, gives a new description of the ideal class group itself.

Section 12 is of a different nature. It is concerned with special radicals, with element resolvents, depending on the elements of a $\mathfrak{p}$-adic number field. An upper bound is

derived for the $\mathfrak{p}$-adic value of element resolvents as functions of elements of the field and characters of its Galois group into a base field. The relationship of element resolvents with Frobenius' group-determinants is pointed out which facilitates the developments of section 12.

I should like to draw the reader's attention to two topics which have not been investigated here though they seem to present promising aspects of the theory.

The characterization of radical modules given in section 3 in purely group- and module-theoretic terms hints at a possible generalization of some of the results involving the ideal class group of a field to the Picard group of a commutative ring. The Picard group is a class group of isomorphism classes of finitely generated projective R-modules and, in the general situation, takes over the role of the ideal class group.

Another aspect opens if one considers together with the fields K and $\overline{K}$ the action of the Galois group $G(\overline{K}/K)$ on the objects we are here concerned with. If, in addition to K, we introduce a finite separable normal extension L of K its Galois group will be isomorphic to $G(\overline{K}/K) \big/ G(\overline{K}/L)$ and one should be able to develop a relative theory of radicals, radical spaces and modules over L and K respectively including the introduction of a relative norm as product of conjugates.

Moreover one might be able to combine both these additional lines of investigation to obtain a theory of radical modules and spaces for Galois-algebras.

I Preliminaries on Radical Spaces and Radical Modules

1. Notation and Definitions

Though radical spaces can be defined in a more general situation (cf [1])we immediately start off with a Dedekind domain o and its quotient field K so that we have the following exact sequences:

$$1 \longrightarrow U(o) \longrightarrow K^* \longrightarrow \mathfrak{P}(o) \longrightarrow 1 \tag{1.1}$$

$$1 \longrightarrow \mathfrak{P}(o) \longrightarrow \mathfrak{J}(o) \longrightarrow \mathfrak{C}(o) \longrightarrow 1$$

where $U(o) \subset o$ is the group of units of o

K^* the multiplicative group of K

$\mathfrak{P}(o) \subset \mathfrak{J}(o)$ the principal and fractional ideals of o

$\mathfrak{C}(o)$ the ideal class group of o.

We exclude from the beginning the case that o is a field. As to radicals, radical spaces, and radical modules we reproduce some of the definitions and elementary facts Fröhlich develops in his paper [1]. For proofs the reader is referred to that paper.

For the following let L be an algebraic extension field of K L^* its multiplicative group, L^+ its additive group also considered as a K-vectorspace. For submodules of L^+ we shall need the module product:

$$M \cdot N = \{\sum \alpha\beta / \alpha \in M,\ \beta \in N\};\ M.N \subset L^+$$

where, of course, only finitely many summands are admitted.

Fröhlich [1] introduces the following definitions (cf. also (2.0), (3.1) of this paper):

(1.2) α radical of L/K $\sim \alpha \in L^*$, $\exists n > 0, n \in \mathbb{N}$, s.th. $\alpha^n \in K^*$.

P radical subspace of $L/K \sim$
(1) P is K-subspace of L^+
(2) P is of K-rank 1
(3) $\exists n > 0$, $n \in \mathbb{N}$, s.th. $P^n = K$

M radical submodule of $L/o \sim$
(1) M non zero finitely generated o-module in L
(2) $\exists$ radical subspace P of L/K s.th. $M \subset P$

For $R(L/K)$, $\mathfrak{r}(L/K)$, $\mathfrak{R}(L/o)$, the sets of all radicals, radical spaces, and radical modules of L over K respectively, the following facts hold:

1) $R(L/K)$, $\mathfrak{R}(L/K)$, $\mathfrak{R}(L/o)$ form abelian groups under field or module multiplication respectively and $R(L/K) \supset K^*$, $\mathfrak{R}(L/o) \supset \mathfrak{F}(o)$.

2) For isomorphic extensions of K the corresponding groups are isomorphic.

The behaviour of these groups under change of L in general is studied in [1], propositions 1.1 and 4.2. These propositions also justify the following conventions.

If $\overline{K}$ is an algebraic closure of K we will write:

$R(K) = R(\overline{K}/K)$ for "the" radicals of K

$\mathfrak{R}(K) = \mathfrak{R}(\overline{K}/K)$ for "the" radical spaces of K

$\mathfrak{R}(o) = \mathfrak{R}(\overline{K}/o)$ for "the" radical modules of K.

which is correct up to isomorphisms.

Using the above mentioned propositions one gets:

(1.3) For an algebraic extension L of K $R(L/K)$, $\mathfrak{R}(L/K)$, $\mathfrak{R}(L/o)$ are isomorphic to subgroups of $R(K)$, $\mathfrak{R}(K)$, and $\mathfrak{R}(o)$ respectively.

2. An Elementary Characterization and some Fundamental Properties of Radicals Modules and Spaces

Radical modules and radical spaces can be characterized in an elementary fashion which yields without much effort some fundamental facts and some of Fröhlich's theorems. Radicals and integral ideals of o suffice to describe both radical spaces and modules as subsets of an algebraic closure $\overline{K}$ of K. We thus avoid reference to intermediate fields.

Denote by $\mathfrak{I}(o)$ the integral ideals in o.

(2.0) Remark:

$$P \in \mathfrak{R}(K) \Leftrightarrow P = \lambda K,\ \lambda \in \mathfrak{R}(K)$$

$$M \in \mathfrak{R}(o) \Leftrightarrow M = \lambda I,\ \lambda \in R(K),\ I \in \mathfrak{J}(o)$$

where $\mathfrak{J}(o)$ denotes the integral ideals in o.

For each K-vectorspace $P \in \mathfrak{R}(K)$ by definition there exists an $n \in \mathbb{N}$ with $P^n = K$; for a generator λ of P we get a fortiori $\lambda^n \in K$, i.e. $\lambda \in R(K)$. Conversely, the objects λK obviously are one-dimensional K-subspaces of K and, if n is the degree of λ, then $(\lambda K)^n = K$, so $\lambda K \in \mathfrak{R}(K)$. Each radical module M by definition is contained in a radical space, say in $P = \lambda K$. Therefore M determines the finitely generated o-module $\lambda^{-1}M$ in K. K being quotient field of the Dedekind domain o its finitely generated o-modules are its fractional ideals and we have

(2.1) $$\lambda^{-1}M = F \text{ or } M = \lambda F,\ F \in \mathfrak{I}(o)$$

F in turn can be written as $F = k I$ with $k \in K$, $I \in \mathfrak{J}(o)$ and therefore $M = (\lambda k)I$, $\lambda k \in R(K)$.

Conversely, the objects λI are submodules of the radical space $\lambda \cdot K$ and as o-modules they are finitely generated I being an ideal in the Dedekind domain o; i.e. $\lambda I \in \mathfrak{R}(o)$.

From this elementary charaterization of radical modules we can read off the following facts.

Radicals and fractional ideals are groups which by (2.1) implies that also $\mathfrak{R}(o)$ is an abelian group containing $F(o)$ as a subgroup (cf. Fröhlich [1], Theorem 4.1).

Another consequence is

(2.2) A radical module as o-module can be generated by at most two elements.

which, by the way, is true for any finitely generated, torsion free module of K-rank 1. Thus we are lead to distinguish radical modules generated over o by one radical only. They form a subgroup of $\mathfrak{R}(o)$ and we will call them principal radical modules and write $\mathfrak{Q}(o)$ for them or $\mathfrak{Q}(L/o)$ if we wish to refer to a subfield L of an algebraic closure of K.

Using this notion we rephrase (2.1) and get:

(2.3) Each radical module $M \in \mathfrak{R}(o)$ is the product a suitable fractional ideal and a principal radical module:

$$M \in \mathfrak{R}(o) \Leftrightarrow M = H \cdot F \quad \text{with} \begin{cases} F \in \mathfrak{F}(o) \\ H \in \mathfrak{Q}(o) \end{cases}$$

Remark: It may be worth noting that $\mathfrak{R}(o)$ is not a direct product of $\mathfrak{F}(o)$ and $\mathfrak{Q}(o)$, but:

$$\mathfrak{R}(o) = \mathfrak{I}(o)\mathfrak{H}(o) \text{ and } \mathfrak{I}(o) \cap \mathfrak{H}(o) = \mathfrak{P}(o) \neq o$$

The analogy of principal radical modules to principal ideals is established by the exactness of the following sequences (cf. sequences (1.1)):

$$1 \longrightarrow U(o) \longrightarrow R(K) \xrightarrow[\alpha \mapsto \alpha o]{} \mathfrak{H}(o) \longrightarrow 1 \tag{2.4}$$

$$1 \longrightarrow \mathfrak{H}(o) \longrightarrow \mathfrak{R}(o) \xrightarrow[\alpha I \mapsto cl(I)]{} \mathfrak{C}(o) \longrightarrow 1$$

As to the exactness of the first sequence we note that the map $\alpha \longrightarrow \alpha o$ is a homomorphism. Its kernel is the set kern $= \{\alpha / \alpha \in R(K),\ \alpha o = o\}$. For these elements α we get:

$$\left.\begin{array}{l} \alpha \in \text{ kern} \Rightarrow \alpha^{-1} \in \text{ kern} \\ \alpha o = o \ \Rightarrow \alpha \in K \text{ and } \alpha \in o \end{array}\right\} \Rightarrow \alpha \text{ is a unit of } o$$

On the other hand: Every $a \in U(o)$ has the property that $ao = o$ which completes the proof.

Considering the second sequence we have in the first place to make sure that the map $\mathfrak{R}(o) \rightarrow \mathfrak{C}(o)$ is well defined by $\alpha I \rightarrow cl(I)$ because our representation of radical modules as product of a radical and an ideal is not unique.

Take $\alpha I,\ \beta J \in \mathfrak{R}(o)$ and assume equality:

$$\alpha I = \beta J \ \Rightarrow \ \alpha\beta^{-1} o = JI^{-1}$$

Going over to the images under cl:

$$cl(o) = cl\,(JI^{-1}) \Leftrightarrow cl(J) = cl(I)$$

which implies $cl(\alpha I) = cl(\beta J)$ proving that our map is well

defined. Later on we shall use "cl" to denote this map and we shall also speak of the class of a radical module.

The exactness of the discussed sequence, however, is obvious regarding that the kernel of the ideal-class-map is $\mathfrak{P}(o)$. The exactness also follows from remark (2.3) by applying Noethers Isomorphism theorem to $\mathfrak{J}(o)\mathfrak{h}(o)$ which yields:

$$\mathfrak{J}(o)\mathfrak{h}(o)/\mathfrak{h}(o) \cong \mathfrak{J}(o)/\mathfrak{J}(o)\cap\mathfrak{h}(o) \Leftrightarrow \mathfrak{R}(o)/\mathfrak{h}(o) \cong \mathfrak{C}(o)$$

Another proof can be found in Fröhlich [1], theorem 5.1. We go along to state relations between radicals, radical modules and radical spaces.

The maps $\quad \alpha \longrightarrow \alpha K$

$\quad\quad\quad \alpha \longrightarrow \alpha o \qquad\qquad$ for $\alpha \in R(K)$

define homomorphisms of groups. The map

$$\lambda I \longrightarrow \lambda IK = \lambda K \qquad \text{of } \mathfrak{R}(o) \longrightarrow \mathfrak{R}(K)$$

is well defined as radicals describing the same radical module differ multiplicatively by an element of K only:

$$\alpha I = \beta J \Rightarrow \alpha\beta^{-1} \in JI^{-1}$$

The commutativity of the following diagram and the exactness of its rows then is obvious:

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^* & \longrightarrow & R(K) & \longrightarrow & \mathfrak{R}(K) & \longrightarrow & 1 \\ & & \Big\downarrow{\scriptstyle a} & & \Big\downarrow & {\scriptstyle \alpha \mapsto \alpha K} & & & \\ & & \Big\downarrow{\scriptstyle ao} & & \Big\downarrow & {\scriptstyle \alpha o} & \| & & \\ 1 & \longrightarrow & \mathfrak{J}(o) & \longrightarrow & \mathfrak{R}(o) & \xrightarrow[\alpha I \mapsto \alpha K]{} & \mathfrak{R}(K) & \longrightarrow & 1 \end{array} \tag{2.5}$$

(cf. also Fröhlich [1],1.1,4.2)

Having considered the group of radical modules $\mathfrak{R}(o)$ modulo $\mathfrak{H}(o)$ and $\mathfrak{F}(o)$ we proceed to determine $\mathfrak{R}(o)/\mathfrak{P}(o)$.

(2.6)The sequence

$$1 \longrightarrow \mathfrak{P}(o) \longrightarrow \mathfrak{R}(o) \longrightarrow \mathfrak{C}(o) \times \mathfrak{R}(K) \longrightarrow 1$$

with $f: \lambda I \mapsto (cl(I), \lambda K)$ is exact.

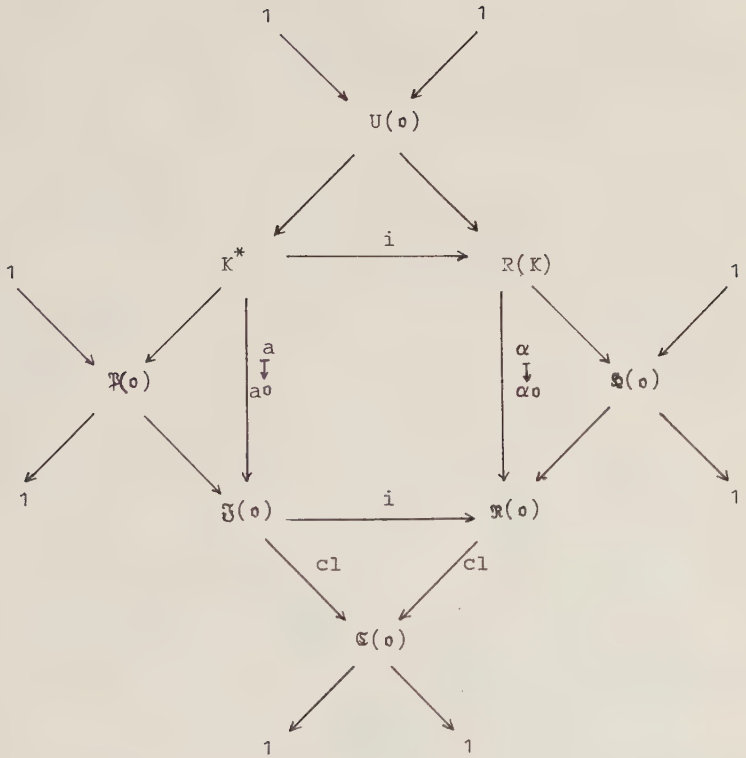
Firstly, both maps $\lambda I \mapsto cl(I)$ and $\lambda I \mapsto \lambda K$ are well defined (cf.(2.4),(2.5)) and therefore so is f.

Secondly, the kernel of f is the intersection of the kernels of the above maps, that is

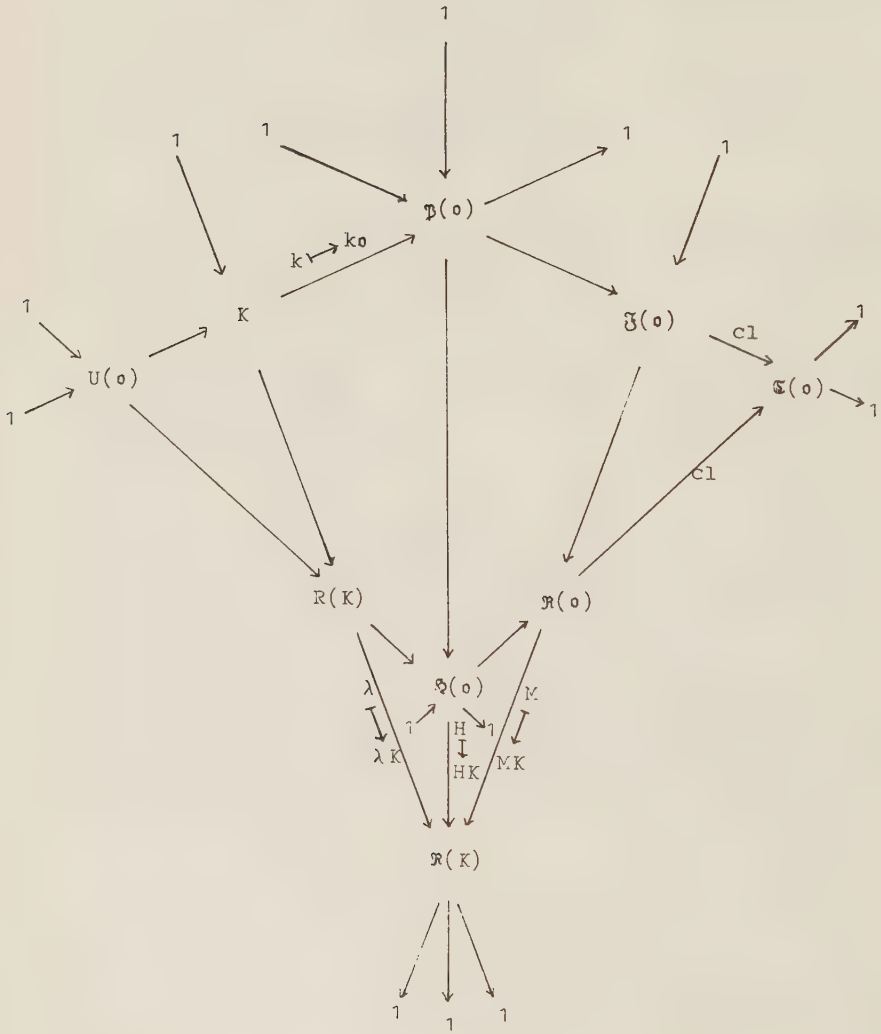
$$\text{kern } f = \mathfrak{H}(o) \cap \mathfrak{F}(o) = \mathfrak{P}(o)$$

Thirdly, f is surjective, for $(cl(I), \lambda K)$ the radical module λJ with $J \in cl(I)$is an original.

To finish this paragraph we combine some of the sequences we have referred to in a diagram to point out the analogy of fractional ideals to radical modules of a field K.
The left hand side consists of the classical sequences, the right hand side involves radicals and radical modules. All four sides of the big square are exact and the maps marked by "i" are injections.


1
1
U(o)
K*
i
R(K)
1
1
$\mathfrak{K}$(o)
a
a_o
α
α_o
$\mathfrak{L}$(o)
1
1
$\mathfrak{J}$(o)
i
$\mathfrak{R}$(o)
cl
cl
$\mathfrak{C}$(o)
1
1

The following diagram links up radicals and radical modules with radical spaces. The diagram commutes and all occurring sequences are exact.



3. Group Theoretic Characterization of Radicals, Radical Spaces, and Modules.

Our aim is to characterize radicals and radical modules with respect to an algebraic closure $\overline{K}$ of K. From diagram (2.5) we obtain for the radical spaces $\mathfrak{R}(K) \cong R(K)/K^*$ showing that up to isomorphism $\mathfrak{R}(K) \subset \overline{K}^*/K^*$. Moreover R(K) turns out to be essentially the torsion part of $\overline{K}^*/K^*$ and R(K) its preimage:

(3.1) $\mathfrak{R}(K) \cong \mathrm{Tor}\,(\overline{K}^*/K^*)$

$R(K) = f^{-1}[\mathrm{Tor}(\overline{K}^*/K^*)]$ under $f: \overline{K}^* \to \overline{K}^*/K^*$

Both statements are immediate consequences of (2.0) or the corresponding definitions and were first pointed out by L.R.Mc.Culloh (Mathematical Reviews 35 # 6660, p 1228).

For the first statement we note that $P \in \mathrm{Tor}\,(\overline{K}^*/K^*)$ means that P is a class $\overline{k}K^*$ and that there exists a natural n with $P^n = K^*$; so a fortiori $\overline{k}^n \in K^*$ will hold i.e. $\overline{k}$ is a radical. The converse is clear.

The second part follows similarly:

$k \in f^{-1}[\mathrm{Tor}(\overline{K}^*/K^*)] \Leftrightarrow k \in \overline{k}\,K^*$ with $\overline{k} \in \overline{K}^*$ and $(\overline{k}K^*)^n = K^*$

i.e. $k^n \in K \Leftrightarrow k \in R(K)$.

On the other hand: $k \in R(K)$, $f(k) = kK^* \in \mathfrak{R}(K)$ by definition.

The importance of (3.1) is that in a straightforward manner it admits a definition of both radicals and radical spaces in entirely group theoretic terms.

We can derive a similar characterization of the group of radical modules as subgroup of finitely generated torsion-free and invertible o-modules $\mathfrak{M}(o)$ in $\overline{K}$ of K-rank 1. The diagram

$$\begin{array}{ccccccccc} 1 & \longrightarrow & K^* & \longrightarrow & \overline{K}^* & \xrightarrow{f} & \overline{K}^*/K^* & \longrightarrow & 1 \\ & & \downarrow k & & \downarrow \alpha & & \downarrow i & & \\ & & ko & & \alpha o & & \alpha K^* & & \\ & & & & & & \downarrow & & \\ & & & & & & \alpha\mathfrak{J}(o) & & \\ 1 & \longrightarrow & \mathfrak{J}(o) & \longrightarrow & \mathfrak{M}(o) & \xrightarrow{g} & \mathfrak{M}(o)/\mathfrak{J}(o) & \longrightarrow & 1 \end{array}$$

is commutative with exact rows. The map $i: \alpha K^* \longrightarrow \alpha\mathfrak{J}(o)$ is an injection. Thus we may view the group of radical spaces $\mathrm{Tor}(\overline{K}^*/K^*) = \mathfrak{R}(K)$ as embedded in $\mathfrak{M}(o)/\mathfrak{J}(o)$ and according to (2.5) $\mathfrak{R}(o)$ turns out to be essentially the preimage of $\mathrm{Tor}(\overline{K}^*/K^*)$ under g:

$$(3.2) \qquad g^{-1}[i[\mathrm{Tor}(\overline{K}^*/K^*)]] = \mathfrak{R}(o)$$

Thus the torsion group of $\overline{K}^*/K^*$ together with the maps f and g provides the means to define radical spaces, radicals, and radical modules as well.

Finally we point out the connection of $\mathfrak{R}(o)$ and $\mathrm{Tor}(\mathfrak{M}(o)/\mathfrak{J}(o))$ and state:

The o-modules $M \in \mathfrak{M}(o)$ satisfying

(3.3)(1) $\dim_K MK = 1$

(2) $M\mathfrak{J}(o) \in \mathrm{Tor}(\mathfrak{M}(o)/\mathfrak{J}(o))$ form the subgroup $\mathfrak{R}(o)$ of $\mathfrak{M}(o)$

The proof bases on the principles we have repeatedly used.

a) $M \in \mathfrak{R}(o) \Rightarrow M = \lambda F$ with $F \in \mathfrak{F}(o)$, $\lambda \in R(K)$

$\Rightarrow MK = \lambda K \Rightarrow \dim_K MK = 1.$

b) $M \in \mathfrak{R}(o) \Rightarrow M = \lambda F$, λ a radical

$\Rightarrow \exists\ n \in \mathbb{N}$ with $M^n \in \mathfrak{J}(o)$

Therefore $(M\mathfrak{J}(o))^n = M^n\mathfrak{J}(o) = \mathfrak{J}(o)$

i.e. $M\mathfrak{J}(o) \in \mathrm{Tor}(\mathfrak{M}(o)/\mathfrak{J}(o))$

Conversely, for any $M \in \mathfrak{M}(o)$ satisfying $M\mathfrak{J}(o) \in \mathrm{Tor}(\mathfrak{M}(o)/\mathfrak{J}(o))$ there exists a natural n with $M^n \in \mathfrak{J}(o)$. Thus M^n is finitely generated over o and therefore M, too. Moreover $M \subset MK$ which because of $\dim_K MK = 1$ is a radical space. According to definition (1.2) M is a radical module and our proof is complete.

We note that o-modules generating over K vector spaces of dimension one form a group. Take $N \in \mathfrak{m}(o)$ $NK = \nu K$, $\nu \in \overline{K}^*$, and consider $NN^{-1} = o$ and $NN^{-1}K = K$. We get $\nu N^{-1}K = K$ or $N^{-1}K = \nu^{-1}K$, i.e. $N^{-1} \in \mathfrak{N}(o)$. For a product $M \cdot N^{-1}$ we obtain, of course, $MN^{-1}K = (\mu\nu^{-1})K$ if $MK = \mu K$, $\mu \in \overline{K}^*$. Thus (3.3) in group theoretic form runs as follows:

$$\mathfrak{R}(o) = \mathfrak{M}(o) \cap \mathfrak{T}(o) \tag{3.4}$$

where $\mathfrak{m}(o) = \{M/M$ o-module in $\overline{K}^*$, $\dim_K MK = 1\}$

and $\mathfrak{r}(o) = g^{-1}[\mathrm{Tor}(\mathfrak{m}(o)/\mathfrak{r}(o))]$.

We may describe the group $\mathfrak{m}(o)$ a little more closely:

$M \in \mathfrak{m}(o) \Rightarrow \dim_K MK = 1$ i.e. $\exists \alpha \in \overline{K}$ with $MK = \alpha K$.

Therefore $\alpha^{-1}M$ is a (finitely generated) o-module in K, that is, a fractional ideal. We may conclude now:

$\alpha^{-1}\, M \in \mathfrak{J}(o) \Rightarrow M = \alpha F,\ F \in \mathfrak{J}(o)$ and get for $\mathfrak{M}(o)$:

$$\mathfrak{M}(o) = \{\alpha F / \alpha \in \overline{K},\ F \in \mathfrak{J}(o)\}$$

showing again that $\mathfrak{M}(o)$ is a group and moreover that its elements are o-modules which can be generated by at most two elements.

4. Summary on Valuations of Radicals, Radical Spaces, and Radical Modules

In § 3 of his paper [1] Fröhlich extends the notion of a valuation of a field K to its group of radicals. We summarize the main facts which will be used here. For a detailed treatment and for proofs we refer the reader to [1].

(4.1) Definition: The function Ψ: $(R(K) \cup o) \to (\mathbb{P} \cup o)$ is called a valuation of $R(K)$ if

(I) the restriction ψ_K of ψ to K is a valuation of K

(II) the restriction of ψ to a radical subspace P is a norm of the K-vector space P with respect to ψ_K

(III) the restriction of Ψ to $R(K)$ defines a homomorphism $R(K) \to \mathbb{P}$

where $\mathbb{P}$ denotes the multiplicative group of positive real numbers.

We shall reproduce the main facts from [1], § 3 in terms of discrete valuations which we shall use preferably. Let $\mathbb{Z}$ denote the additive group of integers and v a discrete exponential valuation $K \to (\mathbb{Z} \cup \infty)$ and $\overline{v}$ its extension to $R(K)$. Then we can state (cf.[1],(3.4)):

(4.2) Every discrete valuation v of K gives rise to a unique valuation $\overline{v}$ of $R(K)$ with $\overline{v}/_K = v$, and the diagram

$$\begin{array}{ccccc} K^* & \longrightarrow & R(K) & \longrightarrow & \mathfrak{R}(K) \\ \downarrow{\scriptstyle v} & & \downarrow{\scriptstyle \overline{v}} & & \downarrow{\scriptstyle \hat{v}} \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}$$ commutes;

$\hat{v}$ being the induced map, it is a character of $\mathfrak{R}(K)$.

As im v = $\mathbb{Z}$ the extension $\overline{v}$ described in [1] maps R(K) onto $\mathbb{Q}$; an element $\alpha \in R(K)$ with $\alpha^n \in K$, $n \in \mathbb{N}$, will get the value $\overline{v}(\alpha) = \frac{1}{n} v(\alpha^n)$. $\overline{v}$ is uniquely determined by v on every subgroup of R(K) containing K^*, and therefore we shall in the sequel use the symbol v also for the extended map.—In the case that K is quotient field of a Dedekind domain o —and we assume this from now on — we can introduce a valuation of radical modules or more generally of any non empty subset S of (R(K) ∪ o) by:

(4.3) Definition: $v^*(S) = \inf_{\sigma \in S} v(\sigma)$

For radical modules we get a diagram similar to that for radicals (cf [1] (4.3)):

(4.4) The diagram

$$\begin{array}{ccccc} \mathfrak{J}(o) & \longrightarrow & \mathfrak{R}(o) & \longrightarrow & \mathfrak{R}(K) \\ \downarrow & v^* & \downarrow & v^* & \downarrow \hat{v} \\ \mathbb{Z} & \longrightarrow & \mathbb{Q} & \longrightarrow & \mathbb{Q}/\mathbb{Z} \end{array}$$ commutes.

And finally we have a commutative diagram linking radicals with radicals modules:

(4.5)

$$\begin{array}{ccc} R(K) & \longrightarrow & \mathfrak{R}(o) \\ & \searrow^{v} \quad \swarrow_{v^*} & \\ & \mathbb{Q} & \end{array}$$ commutes.

This is true because for all $\alpha \in R(K)$ the following equality holds: $v^*(\alpha o) = \inf\{ v(\alpha r) \mid r \in o \} = v(\alpha)$.

For the study of extensions of valuations under the more general conditions of a ring extension the reader is referred to a paper by U. Güntzer (cf. [13] p.173-195).

II. Number-Theoretic Investigations on Radicals and Radical Modules

5. Integral and Unit Elements, a Norm for Radical Modules

Our intention now is to define numbertheoretic concepts for radicals and radical modules by means of valuations. Let K be the quotient field of the Dedekind domain o and $\mathfrak{p}$ a maximal ideal of o. The associated exponential valuation of K and its extension to $R(K)$ shall be denoted by $v_\mathfrak{p}$ and the subscript $\mathfrak{p}$ shall indicate the associated objects to be introduced. $v_\mathfrak{p}^*$ then is the valuation of $\mathfrak{R}(o)$ and, as customary, $o_\mathfrak{p}$ the valuation ring of o, that is the local ring of o at $\mathfrak{p}$ in K.

We observe the following analogy to the field case when considering all maximal ideals $\mathfrak{p}$ of o (cf. Fröhlich [1], (4.4)):

(5.1) Let $\alpha \in R(K)$, $M \in \mathfrak{R}(o)$, $P \in \mathfrak{R}(K)$
Then $v_\mathfrak{p}(\alpha) = 0$, $v_\mathfrak{p}^*(M) = 0$, $\hat{v}_\mathfrak{p}(P) = 0$
for almost all $\mathfrak{p}$.

We proceed to define integral elements of $R(K)$ and of $\mathfrak{R}(o)$.

(5.2) Definition

$\alpha \in R(K)$ integral $\Leftrightarrow v_\mathfrak{p}(\alpha) = 0$ for all $\mathfrak{p}$

$M \in \mathfrak{R}(o)$ integral $\Leftrightarrow v_\mathfrak{p}^*(M) = 0$ for all $\mathfrak{p}$.

We immediately add the remark:

$\alpha \in R(K)$ integral $\Leftrightarrow \exists\, m \in \mathbb{N},\ \alpha^m \in o$

$M \in \mathfrak{R}(o)$ integral $\Leftrightarrow \exists\, n \in \mathbb{N},\ M^n \subset o$.

For an integral radical α with $\alpha^m \in K$, $m \in \mathbb{N}$ we have $v_\mathfrak{p}(\alpha^m) = m\, v_\mathfrak{p}(\alpha) \geq v_\mathfrak{p}(\alpha) \geq 0$ for all $\mathfrak{p}$, i.e. α^m is integral. Vice versa, if $\alpha^m \in K$ is integral then for all $\mathfrak{p}$ we get $v_\mathfrak{p}(\alpha^m) \geq 0$ implying $m \cdot v_\mathfrak{p}(\alpha) \geq 0$ and, as $m \geq 1$, $v_\mathfrak{p}(\alpha) \geq 0$. The second equivalence follows similarly.

We pass on to define unit radicals and unit radical modules

(5.3) Definition:

$$\alpha \in R(K) \text{ unit} \Leftrightarrow v_\mathfrak{p}(\alpha) = 0 \text{ for all } \mathfrak{p}$$
$$M \in \mathfrak{R}(o) \text{ unit} \Leftrightarrow v^*_\mathfrak{p}(M) = 0 \text{ for all } \mathfrak{p}.$$

The units of $R(K)$ form a subgroup which we shall denote by V; it contains the group U of units of o.

Similarly, the units of $\mathfrak{R}(o)$ are a subgroup. We denote it by $\mathfrak{U}(o)$ and have the following inclusions:

$$R(K) \supset V \supset U;\ \mathfrak{R}(o) \supset \mathfrak{U}(o) \supset \{v\}.$$

In terms of integral elements we can rephrase definition (5.3): a radical α is a unit if both α and α^{-1} are integral; an $M \in \mathfrak{R}(o)$ is a unit radical module if both M and M^{-1} are integral. From these global characterizations we immediately deduce the remark:

Remark:

$$\alpha \in V \quad \Leftrightarrow \exists\, m \in \mathbb{N} \text{ such that } \alpha^m \in U$$
$$M \in \mathfrak{U}(o) \Leftrightarrow \exists\, n \in \mathbb{N} \text{ such that } M^n = V$$

If α or M and their inverses are integral then so is any power. This establishes one part of the proof. The other is obvious from (5.3), e.g. take an M with $M^n = o$, then

$$v^*_\mathfrak{p}(M) = \frac{1}{n}\, v^*_\mathfrak{p}(M^n) = 0, \text{ i.e. } M \in \mathfrak{U}(o).$$

The second part of our remark says in group theoretic terms that $\mathfrak{U}(\mathfrak{o})$ is the torsion subgroup of $\mathfrak{R}(\mathfrak{o})$:

$$\mathfrak{U}(\mathfrak{o}) = \mathrm{Tor}\ \mathfrak{R}(\mathfrak{o})$$

Our proof for this fact is more elementary than that given by Fröhlich ([1],7.1).

For later use we will introduce a convenient notation. Let $S \subset K$ be a set of elements of K. Then by R(S) we will denote radicals which stem from S in the following sense:

$$\{\alpha/\alpha \in R(K),\ \exists\, m \in \mathbb{N} \text{ s.th. } \alpha^m \in S\} = R(S) \tag{5.4}$$

m, of course, depending on the individual α. Then we may write $V = R(U)$ and $R(\mathfrak{o})$ coincides with the integral radicals.

The extension of the discrete valuations $v_\mathfrak{p}$ to radicals and radical modules admits the definition of a norm map for radicals extending the classical absolute ideal norm.

For this purpose we assume that the valuations $v_\mathfrak{p}$ are normalized such that

$$v_\mathfrak{p}^*(\mathfrak{p}) = 1 \quad \text{for all } \mathfrak{p}.$$

In this situation we have in the classical case for fractional ideals and their absolute norm the representations

$$\mathfrak{a} = \prod_\mathfrak{p} \mathfrak{p}^{v_\mathfrak{p}^*(\mathfrak{a})}, \qquad n(\mathfrak{a}) = \prod_\mathfrak{p} n(\mathfrak{p})^{v_\mathfrak{p}^*(\mathfrak{a})}$$

for $\mathfrak{a} \in \mathfrak{J}(\mathfrak{o})$ and $n: \mathfrak{J}(\mathfrak{o}) \to \mathbb{P}$ the absolute norm.

We perceive that the formula for the absolute norm is capable of generalization and will provide a suitable definition for an absolute norm for radical modules.

(5.5) Proposition: The map

$$N: \mathfrak{R}(o) \to \mathbb{P} \text{ defined by } M \to \prod_{\mathfrak{p}} n(\mathfrak{p})^{v_{\mathfrak{p}}^*(M)}$$

is a homomorphism extending the ideal norm

$$n: \mathfrak{J}(o) \to \mathbb{P} \quad \text{uniquely.}$$

Proof: N certainly is a homomorphism:

$$\prod n(\mathfrak{p})^{v_{\mathfrak{p}}^*(L\cdot M)} = \prod n(\mathfrak{p})^{v_{\mathfrak{p}}^*(L)+v_{\mathfrak{p}}^*(M)} = \prod n(\mathfrak{p})^{v_{\mathfrak{p}}^*(L)} \cdot \prod n(\mathfrak{p})^{v_{\mathfrak{p}}^*(M)}$$

i.e. $N(L\cdot M) = N(L)\cdot N(M)$ for $L,M \in \mathfrak{R}(o)$.

Moreover, by definition, $N/_{\mathfrak{J}(o)} = n$; that is, it extends n.

The uniqueness of the extension follows from the multiplicativity of N: There is a minimal $m \in \mathbb{N}$ with $M^m \in \mathfrak{J}(o)$ for $M \in \mathfrak{R}(o)$. Then

$$n(M^m) = N(M)^m$$

and, in $\mathbb{P}$, the equation $x^m = n(M^m)$ is uniquely soluble as

$$N(M) = \sqrt[m]{n(M^m)} \tag{5.6}$$

Moreover this is independent of m: For any $m' \in m\mathbb{Z}$ we have

$$\sqrt[m']{n(M^{m'})} = \sqrt[m]{n(M^m)} .$$

One may also conclude the existence and uniqueness of a norm extension from general theory: $\mathbb{P}$ is a torsion free injective $\mathbb{Z}$ - module and therefore there exists a uniquely determined map N which makes the diagram

$$\begin{array}{ccc} \mathfrak{J}(o) & \hookrightarrow & \mathfrak{R}(o) \\ \downarrow{\scriptstyle n} & \swarrow{\scriptstyle N} & \\ \mathbb{P} & & \end{array}$$

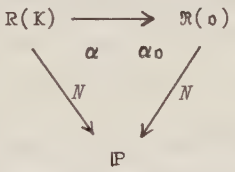
commute (cf.e.g. Kertesz [4]; [12] § 53).

We define the norm of a radical by the norm of the principal radical module it generates using the same symbol N:

(5.7) Definition:

$$N(\alpha) = N(\alpha_0),\ \alpha \in R(K).$$

As $v_p(\alpha) = v_p(\alpha_0)$ for all p we get a commutative diagram involving element and module norm:



6. Examples from Multiplicative Number Theory for Radical Modules

Though our main interest is centred on other questions we will illustrate the notions of integrity and norm of radical modules by providing one or two examples from multiplicative number theory in $\mathfrak{R}(o)$.

For integral radical modules we define divisibility as follows.

(6.1) Definition:

$M, M' \in \mathfrak{R}(o)$ integral

$M/M' \Leftrightarrow M = M'M''$ with $M'' \in \mathfrak{R}(o)$ integral

As usual M' is said to divide M properly if both M' and MM'^{-1} are no unit radical modules.

We note that for integral ideals $\mathfrak{a}, \mathfrak{b}$ we have

$$\mathfrak{a}/\mathfrak{b} \Leftrightarrow \mathfrak{a} \supset \mathfrak{b}.$$

A similar characterization of the divisibility of radical modules is not possible as the modules concerned may come from different radical spaces.

The norm N: $\mathfrak{R}(o) \rightarrow \mathbb{P}$ behaves with respect to divisibility of radical modules as follows:

(6.2) Proposition:

N is a monotonous norm-function:

(1) $L/M \Rightarrow N(L) \leqq N(M)$ for integral L and M

(2) If L is a proper divisor of $M \neq o$ then $N(L) < N(M)$

Proof: $L/M \Rightarrow M = LL'$ where all occurring modules are integral,

i.e. for all $\mathfrak{p}$ the equality

$$v_{\mathfrak{p}}(M) = v_{\mathfrak{p}}(L) + v_{\mathfrak{p}}(L')$$

holds with each summand greater or equal to 0. This yields $v_{\mathfrak{p}}(L) \leqq v_{\mathfrak{p}}(M)$ and therefore

$$n(\mathfrak{p})^{v_{\mathfrak{p}}(L)} \leqq n(\mathfrak{p})^{v_{\mathfrak{p}}(M)}$$

and $$\prod_{\mathfrak{p}} n(\mathfrak{p})^{v_{\mathfrak{p}}(L)} \leqq \prod_{\mathfrak{p}} n(\mathfrak{p})^{v_{\mathfrak{p}}(M)}$$

which proves (1). For part (2) we note that L is no unit i.e. for at least one $\mathfrak{p}$ the value of M is different from that of L which excludes equality in the above formula.

The notion of the norm $N\colon \mathfrak{R}(o) \to \mathbb{P}$ enables us to define Euler's function φ even for radical modules. Let $M \in \mathfrak{R}(o)$ be integral and $P_M = \{\mathfrak{p}/v_{\mathfrak{p}}(M) \neq o\}$. Then the usual formula for ideals provides a means for extending φ to integral radical modules:

(6.3) Definition:

$$\varphi(M) = N(M) \prod_{\mathfrak{p}\in P_M} \left(1 - \frac{1}{n(\mathfrak{p})}\right)$$

As an immediate consequence we get for two integral modules L,M:

$$P_L \cap P_M = \emptyset \Rightarrow \varphi(LM) = \varphi(L)\cdot\varphi(M)$$

One may raise the question whether the extended norm is as in the ideal case summatory function of φ. To see that this is not true we consider a prime ideal $\mathfrak{p}$ and its divisors M (cf.(6.4) below). The infinite series in question $\sum_{M/\mathfrak{p}} \varphi(M)$ consists of terms of the type

$$\varphi(M) = \left(1 - \frac{1}{n(\mathfrak{p})}\right) n(\mathfrak{p})^{\frac{n}{m}}, \quad n < m;\ n, m \in \mathbb{N}$$

They are bounded below by $1 - \frac{1}{n(\mathfrak{p})}$ and therefore their limit will be different from zero. The above series therefore cannot converge. One might investigate whether one or the other limitation method for series yields a result. This is not done here.

Integral radical modules provide an example for a number-theoretic structure with no indecomposable elements (apart from zero).

By (2.0) we reduce this statement to integral ideals and apply a theorem of Fröhlich's (cf [1], Corollary 5.2) saying that for a given ideal I there exists a radical module L with $L^l = I$, $l \in \mathbb{N}$, if and only if $cl(I)$ is an l-th power.

In our case (K algebraic number field) $\mathfrak{C}(o)$ is a finite group and we certainly can represent $cl(I)$ as some suitable power. Having one such representation we immediately can produce infinitely many:

$$cl(I) = cl(F)^l \Rightarrow cl(I) = cl(F)^{l+\nu h}$$

where $\nu = 0,1,2,\ldots$ and $h = |\mathfrak{C}(o)|$, the class-number.

Every exponent $l+\nu h$ gives rise to an L_ν with $L_\nu{}^{l+\nu h} = I$ and each L_ν^m, $0 < m < l+\nu h$, is a divisor of I. Thus we obtain infinitely many divisors of I.

Of special interest, of course, is to get a survey of the divisors of a prime ideal of o. We first derive necessary conditions for such divisors.

Let $\mathfrak{p}$ be a prime ideal in o, $M \in \mathfrak{N}(o)$, and $|M| = m$ shall

denote the smallest natural number such that $M^m \in \mathfrak{J}(o)$.
Then the following statements hold for integral M dividing $\mathfrak{p}$:

(6.4) Lemma:

a) $M/\mathfrak{p} \Rightarrow M^m$ is a power of $\mathfrak{p}$

b) Let $\mathfrak{p} = MM'$ and according to(a): $M^m = \mathfrak{p}^n$, $n \in \mathbb{N}$. Then

(1) $|M| > n$ (for proper divisors)

(2) $|M'| = |M|$

(3) $M'^m = \mathfrak{p}^{m-n}$

Proof: M,M' are integral, $|M| = m$, $|M'| = m'$, and let $k = \text{lcm}[m,m']$. Then

$$\mathfrak{p}^k = (M^m)^{\frac{k}{m}} \cdot (M'^{m'})^{\frac{k}{m'}}$$

is a factorization of $\mathfrak{p}^k$ in o. As $\mathfrak{p}$ is prime it follows that M^m and $M'^{m'}$ are powers of $\mathfrak{p}$ which proves (a).
Moreover:

$$\left.\begin{matrix} MM' = \mathfrak{p} \\ M^m = \mathfrak{p}^n \end{matrix}\right\} \Rightarrow M'^m = \mathfrak{p}^{m-n}$$

which establishes (1) and (3): M' is integral and so is M'^m showing $m > n$, provided M and M' are proper divisors.
Because of $M'^m \in \mathfrak{J}(o)$ we get

$$|M'|/|M|$$

and as M and M' enter symmetrically we also obtain $|M|/|M'|$ and therefore $|M| = |M'| = m$ proving (2).

We are now in a position to formulate a necessary and sufficient condition characterizing the divisors of a prime ideal $\mathfrak{p}$.

(6.5) Proposition: $\mathfrak{p}$ prime ideal in $\mathfrak{o}$; $m,n \in \mathbb{N}$, $m > n$. Then:

$$\mathrm{cl}(\mathfrak{p}^n) \text{ and } \mathrm{cl}(\mathfrak{p}^{m-n}) \text{ are } m\text{-th powers}$$
$$\Leftrightarrow \exists M,M' \in \mathfrak{R}(\mathfrak{o});\ M,M' \text{integral, and } MM' = \mathfrak{p},\ M^m = \mathfrak{p}^n.$$

Proof: Assume that $\mathrm{cl}(\mathfrak{p}^n)$ and $\mathrm{cl}(\mathfrak{p}^{m-n})$ are m-th powers. Then, according to the above cited corollary ([1],5.2) there exist $M,M' \in \mathfrak{R}(\mathfrak{o})$ with

$$\left.\begin{aligned} M^m &= \mathfrak{p}^n \\ M'^m &= \mathfrak{p}^{m-n} \end{aligned}\right\} \Rightarrow (MM')^m = \mathfrak{p}^m$$

from which we deduce $M \cdot M' \cdot \varepsilon = \mathfrak{p}$ where ε is a unit radical by which M' may be modified to get the assertion.
If we start off with a factorization

$$MM' = \mathfrak{p} \text{ with } M^m = \mathfrak{p}^n$$

then by the preceding deliberations (6.4) we obviously have

$$\mathrm{cl}(\mathfrak{p}^n) = \mathrm{cl}(M)^m;\ \mathrm{cl}(\mathfrak{p}^{m-n}) = \mathrm{cl}(M')^m$$

that is, both $\mathrm{cl}(\mathfrak{p}^n)$ and $\mathrm{cl}(p^{m-n})$ are m-th powers.

This proposition shows that we will obtain a complete survey of all divisors of a prime ideal $\mathfrak{p}$ as soon as we know in which cyclic subgroups of the class-group $\mathrm{cl}(\mathfrak{p})$ occurs. More generally, a close knowledge of the structure of the class-group is fundamental to obtain information on all divisors of a given radical module and vice versa.

7. Extension of a Theorem of Minkowski's to Radical Modules

An important consequence of Minkowski's resultful theorem on linear forms ([5], § 6, § 7) is the following :

> Every fractional ideal $F \in \mathfrak{J}(o)$ of an algebraic number field contains an element $a \in F$ such that
>
> $$N(a) \leqq C \cdot N(F)$$
>
> where C is a constant depending on the underlying field only.

Minkowski shows in [5] and [6] that C can be set $C = (\frac{4}{\pi})^{r_2} \cdot \frac{n!}{n} \cdot \sqrt{D}$ where D is the discriminant, n the degree of the underlying field and $2r_2$ the number of its non real conjugate fields over $\mathbb{Q}$.

By combining the notion of the norm of radical modules with remark (2.0) of § 2 we can prove that the above theorem is true not only for fractional ideals but for radical modules of an algebraic number field as well.

Take $M \in \mathfrak{R}(o)$ and write it as

$$M = \alpha F \quad \text{with} \quad \alpha \in R(K),\ F \in \mathfrak{J}(o).$$

Going over to the norms one gets:

$$N(M) = N(\alpha) \cdot N(F).$$

Now apply the above theorem to $F \in \mathfrak{F}(\mathfrak{o})$:

$$C \cdot N(F) \geqq N(a) \quad \text{for some } a \in F$$

$$C \cdot N(M) \geqq N(\alpha) \cdot CN(F) \geqq N(\alpha) \cdot N(a)$$

So we may state:

(7.1) Theorem: Every radical module $M \in \mathfrak{R}(\mathfrak{o})$ contains an element $\mu \in M$ such that

$$N(\mu) \leqq C \cdot N(M)$$

where C is Minkowski's constant.

8. Integral Radical Modules of a Radical Subspace

As vectorspaces over K all radical subspaces are isomorphic. Looking at radical modules, however, we note that in K they form a group, namely the group of fractional ideals, whereas this is not true for the lattice of radical modules of a general radical subspace. But there are strong connections in other respects which we shall establish.

Let us denote by $\mathfrak{R}_P(o)$ the lattice of radical modules of the radical subspace P. $\mathfrak{R}_P(o)$ contains the integral radical modules of P on which our interest will be centred. Fröhlich shows ([1], § 6, § 7) that each radical subspace P contains a unique maximal integral module E_P given by

$$E_P = \{\alpha \in P / v_p(\alpha) \geq o \text{ for all } p\}$$

In order to study $\mathfrak{R}_P(o)$ we define the following map:

$$\mathfrak{F}(o) \longrightarrow \mathfrak{R}_P(o) \text{ by } F \longmapsto F \cdot M_o$$

where M_o is a nontrivial module of P which shall be kept fixed for the following considerations.

This map is a bijection: take $M \in \mathfrak{R}_P(o)$ then $MM_o^{-1} \in \mathfrak{F}(o)$ as both M and M_o are contained in the same P; that is M arises from $F = MM_o^{-1}$; moreover, different M come from different F as $\mathfrak{R}(o)$ is a group.

This bijection is a lattice isomorphism as we have:

$$F_1 \subset F_2 \Leftrightarrow F_1 M_o \subset F_2 M_o$$

$$M_1 \subset M_2 \Leftrightarrow M_1 M_o^{-1} \subset M_2 M_o^{-1}$$

And finally this lattice isomorphism is class-preserving:

$$cl(F_1) = cl(F_2) \Rightarrow cl(F_1M_o) = cl(F_1)cl(M_o)$$
$$= cl(F_2)cl(M_o) = cl(F_2M_o).$$

Especially we realize that in $\mathfrak{R}_P(o)$ there are assembled representatives of all classes of $\mathfrak{C}(o)$.

We summarize these remarks as follows:

(8.1) Lemma: For each radical subspace P and arbitrary but fixed $M_o \in \mathfrak{R}_P(o)$, $M_o \neq P$ the map $\mathfrak{I}(o) \to \mathfrak{R}_P(o)$, $F \mapsto F\,M_o$ is a class-preserving surjective lattice-isomorphism.

By suitable choice of M_o we can for a given radical subspace P produce a still closer connection between $\mathfrak{I}(o)$ and $\mathfrak{R}_P(o)$.

(8.2) Lemma: The map $\mathfrak{I}(o) \to \mathfrak{R}_P(o)$ determined by the maximal integral module E_P of P makes integral ideals correspond biuniquely to the integral radical modules of P.

This is an immediate consequence of the preceding lemma as with o the lattice of its o-submodules corresponds to that of its image which is E_P.

Moreover we note that the norms of an original F and its image M differ by the factor $\mathcal{N}(E_P)$:

$$\mathcal{N}(M) = \mathcal{N}(F) \cdot \mathcal{N}(E_P)$$

because of the multiplicativity of the norm. We are now in a position to provide information about the number of integral radical modules of bounded norm in a radical subspace

over an algebraic number field K.

Let us denote by $T_P(C,t)$ the number of integral radical modules G of P which lie in the class C and have $N(G) \leq t$. Ba lemma (8.1) and (8.2) we conclude:

$$T_P(C,t) = T_K\left(C', \frac{t}{N(E_P)}\right)$$

where $C = C' \cdot cl(E_P)$. Using Dirichlet's and Dedekind's theorems on T_K (cf [9], § 184) we get:

$$\lim_{t\to\infty} \frac{T_P(C,t)}{t} = \lim_{t\to\infty} \frac{T_K\left(C', \frac{t}{N(E_P)}\right)}{t}$$

$$= \frac{1}{N(E_P)} \cdot \lim_{t\to\infty} \frac{T_K\left(C', \frac{t}{N(E_P)}\right)}{\frac{t}{N(E_P)}}$$

$$= \frac{1}{N(E_P)} \cdot \lim_{t'\to\infty} \frac{T_K(C',t')}{t'} = \frac{2^{r_1+r_2}\,\pi^{r_2}}{N(E_P)\sqrt{D(o)}} \cdot \frac{R}{w}$$

where R is the regulator of K

r_1 the number of real infinite places

r_2 the number of complex infinite places

w the order of the group of roots of unity of K^*

D(o) the absolute discriminant of K.

As in the classical case for K we note here for a radical subspace P and its integral radical modules:

1) The number of integral radical modules of norm $N(M) \leq t$ in a given class is of order t.

2) The constant $g_P = \lim_{t\to\infty} \frac{T_P(C,t)}{t}$ is independent of the considered class; that is we have an asymp-

totic equidistribution of integral radical modules of P over the h classes.

Defining the absolute discriminant of a radical module as $D(M) = N(M)^2 \cdot D'(o)$ we state:

(8.3) Theorem: Let P be a radical space over an algebraic number field K,

$C \in \mathfrak{C}(o)$ a class of radical modules,

$T_P(C,t)$ as above,

$T_P(t)$ the number of integral radical modules of P and of norm not greater than t.

Then the following holds:

$$1)\ \lim_{t\to\infty} \frac{T_P(C,t)}{t} = g_P \qquad 2)\ \lim_{t\to\infty} \frac{T_P(t)}{t} = g_P \cdot h$$

where $g_P = \frac{2^{r_1+r_2}\pi^{r_2}}{\sqrt{D(E_P)}} \cdot \frac{R}{w}$ and h is the class number.

Finally we remark that by similar considerations we can extend the lemma on which the proof of the above results in their classical form bases:

(8.4) Lemma: $\lim_{t\to\infty} \frac{T_G(t)}{t} = \frac{2^{r_1+r_2}\pi^{r_2}}{\sqrt{D(G)}} \cdot \frac{R}{w}$

where G is an integral radical submodule of P

$T_G(t)$ the number of principal radical submodules of G of norm not greater than t.

III. Radicals over Local Fields

9. The Valuation Maps v, v^*, $\hat{v}$

For this and the following section 10 let K be quotient field of a discrete valuation ring o with maximal ideal $\mathfrak{p}$, that is $o = o_{\mathfrak{p}}$. We assume the associated valuation $v = v_{\mathfrak{p}}$ of K to be normalized such that $v^*(\mathfrak{p}) = 1$. $V_{\mathfrak{p}}$, $U_{\mathfrak{p}}$, and $U(o_{\mathfrak{p}})$ are the local objects corresponding to the groups introduced in section 5.

The aim of the present section is to obtain information about v, v^*, $\hat{v}$ viewed as homomorphisms from the multiplicative groups $R(K)$ respectively $R(o)$ into the additive group $\mathbb{Q}$ of the rationals.

We shall use repeatedly an elementary lemma on exact sequences of modules over a ring A (cf [7]. III, Lemma 3.3).

(9.0) Lemma: The commutative diagram of A-modules and homomorphisms with exact rows

$$\begin{array}{ccccccccc} o & \longrightarrow & M' & \xrightarrow{\mu'} & M & \xrightarrow{\mu} & M'' & \longrightarrow & o \\ & & \downarrow{\scriptstyle f'} & & \downarrow{\scriptstyle f} & & \downarrow{\scriptstyle f''} & & \\ o & \longrightarrow & N' & \xrightarrow[\nu']{} & N & \xrightarrow[\nu]{} & N'' & \longrightarrow & o \end{array}$$

gives rise to an exact sequence:

$$o \to \operatorname{kern}(f') \xrightarrow{\overline{\mu}'} \operatorname{kern}(f) \xrightarrow{\overline{\mu}} \operatorname{kern}(f'') \xrightarrow{\delta} \operatorname{cok}(f') \xrightarrow{\overline{\nu}'} \operatorname{cok}(f) \xrightarrow{\overline{\nu}} \operatorname{cok}(f'') \to o$$

where $\overline{\mu}'$, $\overline{\mu}$ are restrictions of μ', μ

$\overline{\nu}'$, $\overline{\nu}$ are induced by ν', ν

and the boundary homomorphism δ is defined as follows.

If $x'' \in \operatorname{kern}(f'')$ then the following equations will hold:

$x'' = \mu(x)$ for some $x \in M$, and $\nu(f(x)) = f''(\mu(x)) = o$ hence $f(x) \in \ker(\nu) = \mathrm{im}(\nu')$, i.e. $f(x) = \nu'(y')$ for some $y' \in N'$. Then $\delta(x'')$ is defined to be the image of y' in $\mathrm{cok}(f')$.

(9.1) Proposition: The following sequences are exact:

$$1 \to V_p \to R(K) \xrightarrow{v} \mathbb{Q} \to o$$

$$1 \to U(o_p) \to \mathfrak{R}(o) \xrightarrow{v^*} \mathbb{Q} \to o$$

Proof: In connection with (4.2) and (4.5) we have already seen that both $R(K)$ and $\mathfrak{R}(o)$ are mapped into $\mathbb{Q}$ by v and v^* respectively.

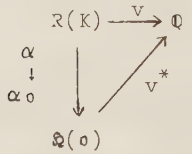
The kernel of v consists of radicals α with $v(\alpha) = o$, by definition, this V_p. Similarly we have for the kernel of v^*:

$$\ker v^* = \{M/M \in \mathfrak{R}(o),\ v^*(M) = o\} = U(o_p)$$

To show surjectivity of v we consider $\frac{m}{n} \in \mathbb{Q}$ with the intention to provide a radical with value $\frac{m}{n}$. Take $\pi \in K$ with $v(\pi) = 1$ and choose a radical α defined by $x^n - \pi^m = o$. Then

$$v(\alpha) = \frac{1}{n}\ v(\pi^m) = \frac{m}{n}\ .$$

For surjetivity of v^* we look at the commutative diagram:



Apart from v^* all maps are known to be surjective, therefore $v^*: \mathfrak{Q}(o) \to \mathbb{Q}$ is surjective, too. $\mathfrak{Q}(o)$ and $\mathfrak{R}(o)$ coincide as we are in the local case, hence v^* is surjective.—By the way, the second sequence of (9.1) can be obtained by interpreting the first one in terms of principal radical modules.

To complete the picture we note that for the elements of a radical space $P = \alpha K$ we get $v\colon P \to v(\alpha) + \mathbb{Z}$. Especially, a radical space $P = \alpha K$ is mapped onto $\mathbb{Z}$ under v if the generator α of the space has the property $v(\alpha) \in \mathbb{Z}$.

(9.2) Proposition: The following sequence is exact:

$$1 \to U(o_p) \to \mathfrak{R}(K) \xrightarrow{\hat{v}} Q/\mathbb{Z} \to o$$

Moreover: $\ker \hat{v} = U(o_p) \cong V_p)/U_p$

Proof: Firstly apply lemma (9.o) to

$$\begin{array}{ccccccc} 1 & \to & \mathfrak{J}(o) & \to & \mathfrak{R}(o) & \to & \mathfrak{R}(K) \to 1 \\ & & \downarrow & & \downarrow v^* & & \downarrow \hat{v} \\ o & \to & \mathbb{Z} & \to & Q & \to & Q/\mathbb{Z} \to o \end{array}$$

which commutes and has exact rows (cf(4.4)). As in the local case $v^*/_{\mathfrak{J}(o)}\colon \mathfrak{J}(o) \to \mathbb{Z}$ is a bijection ($\mathfrak{J}(o)$ infinite cyclic) we get the following exact sequence:

$$1 \to \ker v^* \to \ker \hat{v} \xrightarrow{\delta} o \to o \to \operatorname{cok} \hat{v} \to o$$

yielding together with (9.1):

$$\ker \hat{v} \cong \ker v^* \cong U(o_p)$$
$$\operatorname{cok} \hat{v} \cong \operatorname{cok} v^* = o$$

In other words, $\hat{v}$ is surjective and

$$1 \to U(o_p) \to \mathfrak{R}(K) \to Q/\mathbb{Z} \to o \text{ exact.}$$

Secondly, apply the same considerations to

$$\begin{array}{ccccccc} 1 & \to & K^* & \to & R(K) & \to & \mathfrak{R}(K) \to 1 \\ & & \downarrow & & \downarrow v^* & & \downarrow \hat{v} \\ o & \to & \mathbb{Z} & \to & Q & \to & Q/\mathbb{Z} \to o \end{array}$$

which by (4.2) is commutative with exact rows.

Then (9.0) yields that

$$1 \longrightarrow U_{\mathfrak{p}} \longrightarrow V_{\mathfrak{p}} \longrightarrow \operatorname{kern} \hat{v} \longrightarrow o$$

is exact, that is

$$\operatorname{kern} \hat{v} \cong V_{\mathfrak{p}}/U_{\mathfrak{p}}$$

which proves the second part of (9.2).

10. On the Structure of R(K) for Locally Complete K

In the preceding section we established the exact sequence

$$1 \to V_{\mathfrak{p}} \to R(K) \xrightarrow{v} \mathbb{Q} \to o \ .$$

Shifting our attention from the homomorphism v to the groups involved we shall be able to provide some information on the structure of R(K).

We remark that because of (2.4) in the local case we have $\mathfrak{R}(o) \cong R(K)/U(o)$. Hence it will suffice to consider R(K).

We at first concentrate on its subgroup $V_{\mathfrak{p}}$ and derive for it a slightly different characterization which will be helpful as we go along. Let $U_1 = 1 + \mathfrak{p}$ denote the one - units of K, then U_1 is a subgroup of $U_{\mathfrak{p}}$ and for the radicals stemming from U_1 we get:

(10.1) $R(U_1) = R(U_{\mathfrak{p}}) = V_{\mathfrak{p}}$ if the residue class field is algebraic over a finite field.

Proof: Firstly we set out to show $R(U_{\mathfrak{p}}) \subset R(U_1)$.
$\alpha \in R(U_{\mathfrak{p}}) \Rightarrow \exists\ m$ such that $\alpha^m \in U_{\mathfrak{p}}$. We write α^m in its $\mathfrak{p}$-adic representation:

$$\alpha^m = a_o + a_1 \pi + \ldots \text{ with } v_{\mathfrak{p}}(\pi) = 1.$$

Because α^m is a unit $a_o \neq o$ and therefore there exists a $t \in \mathbb{N}$ with $a_o^t \equiv 1(\pi)$. So we get: $\alpha^{mt} \in U_1$ and $\alpha \in R(U_1)$. Secondly we deduce from $U_1 \subset U_{\mathfrak{p}}$ that also $R(U_1) \subset R(U_{\mathfrak{p}})$ which completes the proof of the lemma.

Roughly we may say that $V_{\mathfrak{p}}$ takes over the role of both of units and one-units in our context.

One can carry this a little further. For each $n \geq 1$ the

set $U_n = 1 + \mathfrak{p}^n$ is a subgroup of $U_\mathfrak{p}$ and we have a chain:

$$U_1 \supset U_2 \supset \ldots \supset U_n \supset \ldots$$

This carries over to the corresponding radicals:

$$R(U_1) \supset R(U_2) \supset \ldots \supset R(U_n) \supset \ldots$$

On the other hand, if p is the characteristic of the residue class field, one has

$$U_n^p \subset U_{n+1} \text{ for all } n \geq 1 \text{ (cf.[8],p6,prop.5)}$$

Therefore $R(U_n^p) \subset R(U_{n+1})$. But clearly $R(U_n^p) = R(U_n)$, so we arrive at

$$R(U_1) \subset R(U_2) \subset \ldots \subset R(U_n) \subset \ldots$$

which together with the above chain yields equality

$$R(U_1) = R(U_2) = \ldots = R(U_n) = \ldots$$

The same argument goes through already with forming radicals of prime power degree only.

Write P_n for the set

$$P_n = \{\alpha / \alpha \in R(K) \ , \ \exists\, \nu \in \mathbb{Z} \text{ s.th. } \alpha^{p^\nu} \in U_n\}.$$

Then P_n is a subgroup and by the above considerations $P_n = P_{n+1}$ for all n. We state these remarks in

(10.2) Lemma: The groups $U_n = 1+\mathfrak{p}^n$, $n \geq 1$, give rise to the equalities

$$R(U_1) = R(U_2) = \ldots = R(U_n) = \ldots$$

$$P_1 = P_2 = \ldots = P_n = \ldots$$

provided the residue class field is of prime characteristic.

We introduce the additional assumption that K is a p-adic

number field, that is a field of characteristic zero, complete with respect to the discrete valuation v, and with finite residue class field $o/\mathfrak{p}$ where $\mathfrak{p}$ is the maximal ideal belonging to v. By e we denote the absolute ramification index: $e = v(p)$, $(p) = \mathfrak{p} \cap \mathbb{Z}$.

Under this assumption one can provide a theory of power series over K which was first given by Kurt Hensel (cf [11] chapter 7); for a more up to date account see e.g. [10] § 17). We list the facts needed here.

There is a $\mathbb{Z}$-homomorphism from U_1 into K^+ defined by the logarithm:

$$\log: U_1 \longrightarrow K^+, \quad a \longmapsto \sum_{n=1}^{\infty} (-1)^{n-1} \frac{(a-1)^n}{n}$$

The domain of convergence of log x is exactly U_1. Moreover, one can find a subgroup of U_1 for which log induces an injection:

Let $\overline{e} = \left[\frac{e}{p-1} \right] + 1$, then

$$\log: U_{\overline{e}} \longrightarrow (\mathfrak{p}^{\overline{e}})^+$$

is an isomorphism and

$$v_p(\log u) = v_p(u - 1) \text{ for } u \in U_{\overline{e}} .$$

The inverse map is given by the exponential series:

$$\exp: (\mathfrak{p}^{\overline{e}})^+ \rightleftarrows U_{\overline{e}} \quad , \quad a \longmapsto \sum_{n=0}^{\infty} \frac{a^n}{n!}$$

The domain of convergence of exp x is exactly $(\mathfrak{p}^{\overline{e}})^+$.

We return now to the investigation of the group V_p of unit radicals which contains U_1. Our aim is to extend

the homomorphism log to a homomorphism of V_p thus providing a tool for further studies.

(10.3) Proposition:

(I) There exists a uniquely determined homomorphism

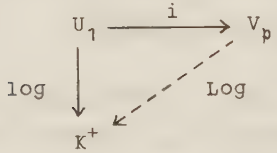
$$\mathrm{Log}: V_p \to K^+$$

such that $\mathrm{Log}/_{U_1} = \log$.

(II) For $\alpha \in V_p$ with $\alpha \in U_1$ the image of α is given explicitly by

$$\mathrm{Log}\ \alpha = \frac{1}{h} \log \alpha^h$$

Proof: In the diagram of abelian groups



K^+ is the additive group of a field of characteristic zero. It is, therefore, a torsion free divisible and consequently injective abelian group (cf e.g. [12],p 247). Hence the homomorphism log can be extended to V_p uniquely.

For $\alpha \in V_p$ there exists according to (11.1) an $h \in \mathbb{N}$ such that $\alpha^h \in U_1$. By the homomorphism - property of Log we obtain

$$\mathrm{Log}\,\alpha = \frac{1}{h}\ \mathrm{Log}\ \alpha^h = \frac{1}{h} \log \alpha^h$$

which proves (II).

We are entering now into a more detailed discussion of the homomorphism Log.

It will prove to be surjective and its kernel will be determined as the group of roots of unity which we shall denote by W.

(10.4) Proposition: The following is an exact sequence of abelian groups:

$$1 \to W \to V_{\mathfrak{p}} \xrightarrow{\text{Log}} K^+ \to o$$

Proof: a) The kernel of Log: $V_{\mathfrak{p}} \to K^+$.

Take a $\xi \in V_{\mathfrak{p}}$. By lemma (11.1) there exists a natural number h such that $\xi^h \in U_1$, and for the logarithms we have $\log u = h \cdot \text{Log}\, \xi$. Assume ξ to be in the kernel of Log, then $\log u = o$. This implies $u^{p^\nu} = 1$ for suitable $\nu \in \mathbb{N}$ (cf [10] § 17.4), that is $\xi^{h \cdot p^\nu} = 1$, ξ is a root of unity. On the other hand, let $\xi \in W$, then $\xi^h = 1$ for a suitable $h \neq o$ and $\text{Log}\, \xi = \frac{1}{h} \log 1 = o$.

b) Surjectivity: We remember that log induces a $\mathbb{Z}$-homomorphism: $U_{\overline{e}} \cong (\mathfrak{p}^{\overline{e}})^+$. Passing to Log we get denominators in the image:

$$\text{Log}[V_{\mathfrak{p}}] \supset \frac{1}{h} (\mathfrak{p}^{\overline{e}})^+ \text{ for all } h \in \mathbb{N}.$$

Especially, if π is a generator of $\mathfrak{p}$, $\pi^{em} = p^m$, $m \in \mathbb{N}$ will turn up as denominators and therefore

$$\text{Log}[V_{\mathfrak{p}}] \supset \bigcup_{m=o}^{\infty} \pi^{-em} (\mathfrak{p}^{\overline{e}})^+ = K^+$$

so all of K^+ appears as image.

Remarks:

1) For the one-units of K the corresponding

sequence is (cf [10], § 15.5 and § 17.5):

$$o \longrightarrow W_p \longrightarrow U_1 \longrightarrow o_p^+ \longrightarrow o$$

W_p denotes the p^{th}-roots of unity in K. This sequence splits because $o_p \cong (p^{\overline{e}})^+$ and $\exp\left[(p^{\overline{e}})^+\right] \to U_1$ provides a map with the property $\log \cdot \exp = id_{o_p}$.

Unfortunately the situation is different in our context of radicals. One cannot prove that the sequence of proposition (10.3) splits.

2) The preceding considerations show that already the subgroup $P \subset V_p$ of radicals of prime power degree is being mapped surjectively onto K^+:

$$P \xrightarrow{\text{Log}} K^+ \longrightarrow o \quad \text{is exact}$$

3) As a final remark we refer to a question of Hasse's([10] § 17.4) asking for a non-archimedean analogue to the transcendental number e. We in fact can determine here radicals ε with the property $\text{Log } \varepsilon = 1$. We first derive necessary conditions.

Assume $\varepsilon \in V_p$ with $\text{Log } \varepsilon = 1$. By lemma (10.1) there exists an $h \in \mathbb{N}$ such that $\varepsilon^h \in U_1$. Then $\text{Log } \varepsilon = \frac{1}{h} \log \varepsilon^h = 1$. This yields two conditions:

a) $\log \varepsilon^h \in p^{\overline{e}} \Rightarrow h \in p^{\overline{e}}$

b) $\log \varepsilon^h = h \Rightarrow \varepsilon^h = \exp h$ by (a),

that is ε satisfies the equation

$$\varepsilon^h - \exp h = o.$$

One verifies now easely the following

(10.5) Corollary: Every $h \in \mathfrak{p}^{\overline{e}} \cap \mathbb{Z}$ gives rise to h radicals whose logarithm is equal to 1. They are defined by $x^h - \exp h = 0$.

For example $h = p$ satisfies the above conditions: $p = \pi^e$ (e here indicates again the absolute ramification index), therefore $p \in \mathfrak{p}^{\overline{e}}$ and, of course, $p \in \mathbb{N}$. So $x^p - \exp p = 0$ defines radicals ε with

$$\operatorname{Log} \varepsilon = \frac{1}{p} \log \varepsilon^p = \frac{1}{p} \log(\exp p) = 1.$$

The one-unit $\exp p$ is given by the series:

$$\exp p = \sum_{n=0}^{\infty} \frac{p^n}{n!}$$

Finally we summarize the results of this paragraph:

The group $R(K)$ of radicals over a complete $\mathfrak{p}$-adic number field has the following chain of subgroups:

$$R(K) \supset V_p \supset W \supset 1$$

The corresponding factor groups are:

$$R(K)/V_p \cong \mathbb{Q}^+, \quad V_p/W \cong K^+, \quad W \cong \mathbb{Q}/\mathbb{Z}.$$

IV. Global and p-adic Applications

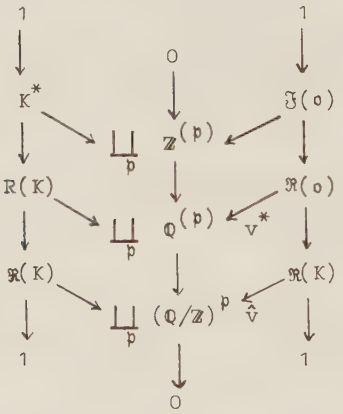
11. Global Maps Induced by Valuations and the Ideal Class Group

We return to the situation that K is the quotient field of a Dedekind domain $\mathfrak{o}$. The discrete valuations determined by maximal ideals $\mathfrak{p}$ of $\mathfrak{o}$

$$v_{\mathfrak{p}}: R(K) \longrightarrow \mathbb{Q} \qquad v_{\mathfrak{p}}^{*}: \mathfrak{R}(\mathfrak{o}) \longrightarrow \mathbb{Q} \qquad \hat{v}_{\mathfrak{p}}: (\mathfrak{R}(K) \longrightarrow \mathbb{Q}/\mathbb{Z}$$

give rise to the following maps:

(11.1)



$\coprod$ stands for the restricted direct product of groups. For exactness of the columns cf.(4.2) and (4.4).

It is our intention to study these maps more closely. We shall determine the kernels and cokernels of these maps. Applying the results to the case of algebraic number fields we shall obtain a characterization of the ideal class group as factor group of the unit radical modules which has

no analogue in the classical theory.

Firstly we look at the kernels of the maps under consideration. $\alpha \in$ kern v means $\alpha \in$ kern v_p for all p, so by definition (5.3) kern v = V. Similarly we get kern v^* = $\mathfrak{U}(o)$ by (5.3).

To obtain kern $\hat{v}$ we apply lemma (9.0) to the right hand side of diagram (11.1):

$$\begin{array}{ccccccccc} 1 & \longrightarrow & \mathfrak{J}(o) & \longrightarrow & \mathfrak{R}(o) & \longrightarrow & \mathfrak{R}(K) & \longrightarrow & 1 \\ & & \downarrow & & \downarrow & & \downarrow & & \\ 0 & \rightarrow & \coprod_p \mathbb{Z}^{(p)} & \rightarrow & \coprod_p \mathbb{Q}^{(p)} & \rightarrow & \coprod_p \mathbb{Q}/\mathbb{Z}^p & \rightarrow & 0 \end{array}$$

Because of the exactness of its rows we get an exact sequence (note that $\mathfrak{J}(o) \cong \coprod \mathbb{Z}^{(p)}$)

$$1 \longrightarrow \text{kern } v^* \longrightarrow \text{kern } \hat{v} \rightarrow o \rightarrow \text{cok } v^* \longrightarrow \text{cok } \hat{v} \rightarrow o$$

which yields for the kernels and cokernels involved:

$$\begin{aligned} \text{kern } \hat{v} &\cong \text{kern } v^* \\ \text{cok } \hat{v} &\cong \text{cok } v^* \end{aligned} \tag{11.2}$$

This proves the first part of

(11.3) Theorem:

(I) $\quad \text{kern } v = V$

$\quad\quad \text{kern } \hat{v} \cong \text{kern } v^* = \mathfrak{U}(o)$

(II) $\quad \text{cok } v \cong \mathbb{Q} \otimes_{\mathbb{Z}} \mathfrak{C}(o)$

$\quad\quad \text{cok } \hat{v} \cong \text{cok } v^* \cong \mathbb{Q} \otimes \mathfrak{C}(o)/\mathbb{Z} \otimes \mathfrak{C}(o)$

We are left with the proof of the second part and first turn to the map v. It maps R(K) into $\coprod_p \mathbb{Q}^{(p)}$ which can be written differently:

$$\coprod \mathbb{Q}^{(p)} \cong \coprod (\mathbb{Q} \otimes \mathbb{Z})^{(p)} = \coprod (\mathbb{Q} \otimes \mathbb{Z}^{(p)} \cong \mathbb{Q} \otimes \coprod \mathbb{Z}^{(p)}$$

On the other hand we have $\coprod \mathbb{Z}^{(p)} \cong \mathfrak{J}(o)$ and thus may write:

$$v: \quad R(K) \longrightarrow \mathbb{Q} \otimes_{\mathbb{Z}} \mathfrak{J}(o)$$

We consider another map ψ which also goes into $\mathbb{Q} \otimes \mathfrak{J}(o)$; it is the map induced by tensoring $K^* \longrightarrow \mathfrak{J}(o)$ with $\mathbb{Q}^+$, all groups considered as $\mathbb{Z}$-modules. For further reference we write down the corresponding commutative diagram and denote the maps involved by ψ_o and ψ, φ and ω.

(11.4)
$$\begin{array}{ccc} K^* & \xrightarrow{\psi_o} & \mathfrak{J}(o) \\ \downarrow{\scriptstyle \varphi} & & \downarrow{\scriptstyle \omega} \\ \mathbb{Q} \otimes K^* & \xrightarrow{\psi} & \mathbb{Q} \otimes \mathfrak{J}(o) \end{array}$$

Thus we have the following diagram:

(11.5)
$$\begin{array}{ccc} R(K) & & \\ & \searrow^{v} & \\ & & \mathbb{Q} \otimes \mathfrak{J}(o) \\ \mathbb{Q} \otimes K^* & \nearrow_{\psi} & \end{array}$$

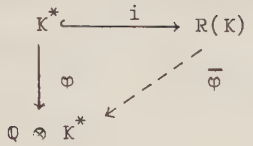
The idea now is to show that $\mathrm{im}(v) = \mathrm{im}(\psi)$ which will imply equality of the cokernels of both maps.

For this purpose we construct a surjective map

$$\Theta: \quad R(K) \longrightarrow \mathbb{Q} \otimes K^*$$

such that it makes diagram (11.5) commute.

In the diagram



i is an injection. $\mathbb{Q}$ is a torsion free and divisible $\mathbb{Z}$-module. Therefore (cf. [7], VII, prop.1.4) the same is true for $\mathbb{Q} \otimes_{\mathbb{Z}} K^*$. For $\mathbb{Z}$-modules however divisibility and injectivity are equivalent and hence φ can be extended in a unique manner to $\bar{\varphi}$ defined on R(K).

We take $\Theta = \bar{\varphi}$ and assert:

$$\Theta \text{ is surjective and } v = \psi \circ \Theta$$

Surjectivity: We write R(K) multiplicatively and $\mathbb{Q} \otimes K^*$ additively the latter viewed as $\mathbb{Q}$-module.

Given $\frac{p}{q} \otimes c \in \mathbb{Q} \otimes_{\mathbb{Z}} K^*$ with $c \in K^*$, $p, q \in \mathbb{Z}$, $q \neq 0$ then $\frac{p}{q} \otimes c = \frac{1}{q} \quad (1 \otimes c^p)$.

We assert that this is the image of $\alpha \in R(K)$ with $\alpha^q = c^p \in K$. For this we get

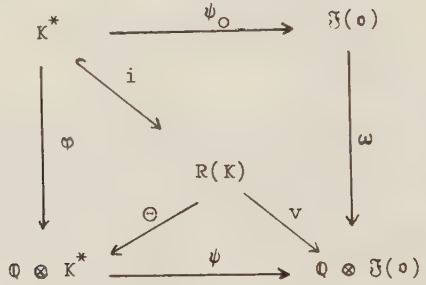
$$\Theta(\alpha^q) = \Theta \circ i\,(c^p) = 1 \otimes c^p$$

$$\left.\begin{array}{l} q\,\Theta(\alpha) = 1 \otimes c^p \\ \mathbb{Q} \otimes K^* \text{ torsionfree} \end{array}\right\} \Rightarrow \Theta(\alpha) = \frac{1}{q}\,(1 \otimes c^p)$$

q.e.d.

Commutativity relation $v = \psi \circ \Theta$:

To show this we embed diagram (11.4) into a bigger one, namely (11.5):



The following parts of this diagram commute:

$\Theta \circ i = \varphi$ by definition of Θ

$\psi \circ \varphi = \omega \circ \psi_o$ as ψ is defined as induced by ψ_o

$\omega \circ \psi_o = v \circ i$ because $\omega \circ \psi_o = v/_{K^*}$

We first show the validity of $v = \psi \circ \Theta$ for elements of K:

$$\psi \circ \Theta \circ i = \psi \circ \varphi = \omega \circ \psi_o = v \circ i$$

by the above relations.

Secondly we consider elements $\alpha \in R(K)$.

For α with $\alpha^n = a \in K$ we get:

$$\left.\begin{array}{l} n\,(\psi \circ \Theta(\alpha) - v(\alpha)) \\ = \psi \circ \Theta\,(ia) - v(ia) = o \\ \mathbb{Q} \otimes \mathfrak{J}(o) \text{ is torsion free} \end{array}\right\} \Rightarrow \psi \circ \Theta(\alpha) = v(\alpha)$$

which holds for all $\alpha \in R(K)$ and hence it proves the commutativity of (11.5) completed by Θ:

We may now conclude as follows:

$$\left.\begin{array}{l}\Theta \text{ surjective} \Rightarrow \operatorname{im}(\psi \circ \Theta) = \operatorname{im}(\psi) \\ \text{commutativity: } \psi \circ \Theta = v\end{array}\right\} \Rightarrow \operatorname{im}(v) = \operatorname{im}(\psi)$$

which in turn yields cok v = cok ψ

The latter can be read from the sequence

$$Q \otimes K^* \longrightarrow Q \otimes \mathfrak{Z}(o) \longrightarrow Q \otimes \mathfrak{C}(o) \longrightarrow 1$$

which is exact as the tensor product is right exact.
Hence cok $v \cong Q \otimes \mathfrak{C}(o)$ and

$$1 \to V \to R(K) \xrightarrow{v} \coprod Q^{(p)} \to Q \otimes \mathfrak{C}(o) \to 1$$

is exact.

It remains to determine the cokernels of v^* and $\hat{v}$. From (11.2) we already know their equality. So it will be sufficient to obtain cokern $\hat{v}$.
We apply lemma (9.0) to the left hand part of (11.1), namely to

$$\begin{array}{ccccccc} 1 & \longrightarrow & K^* & \longrightarrow & R(K) & \longrightarrow & \mathfrak{R}(K) \longrightarrow 1 \\ & & \downarrow & & \downarrow & & \downarrow \\ o & \to & \coprod \mathbb{Z}^{(p)} & \to & \coprod Q^{(p)} & \to & \coprod (Q/\mathbb{Z})^p \to o \end{array}$$

and get the following exact sequence:

$$(11.6) \quad 1 \to U \to V \to U(o) \xrightarrow{\delta} \mathfrak{C}(o) \xrightarrow{\gamma} Q \otimes \mathfrak{C}(o) \to \operatorname{cok} \hat{v} \to o$$

where δ denotes the connecting homomorphism. This sequence provides the desired result. As im (γ) = $= \mathbb{Z} \otimes \mathfrak{C}(o)$ we get for cok $\hat{v}$:

$$\operatorname{cok} \hat{v} = Q \otimes \mathfrak{C}(o) \Big/ \mathbb{Z} \otimes \mathfrak{C}(o)$$

proving the last assertion of theorem (11.3).

For torsion free $\mathfrak{C}(o)$ this quotient is isomorphic to $\mathbb{Q}/\mathbb{Z} \otimes \mathfrak{C}(o)$ (cf [7] Prop.2.3).

The connecting homomorphism δ of sequence (11.6) played a merely auxiliary role up to now. But it presents in itself an interesting feature of the theory. Namely, we shall be able to identify $\delta: U(o) \to \mathfrak{C}(o)$ in terms of the class map cl.

For this purpose we give a more detailed description of δ. Let M be a unit radical module. Its image in $\mathfrak{R}(K)$ is the radical space MK (cf.2.2) which by definition can be represented as $MK = \alpha K$ with suitable radical $\alpha \in R(K)$. By definition $\delta(M)$ is the class of the ideal determined by $v(\alpha)$.

The application of (2.3) to M provides us with another description of $v(\alpha)$: M has a representation as $M = F \cdot \alpha o$ with $F \in \mathfrak{I}(o)$, $\alpha o \in \mathfrak{P}(o)$. Moreover: $M \in U(o)$ means $v^*(M) = o$. Putting this together we get:

$$\left.\begin{aligned} v^*(F) + v^*(\alpha o) &= o \quad \text{or} \quad v^*(\alpha o) = -v^*(F) \\ v^*(\alpha o) &= v(\alpha) \\ -v^*(F) &= v^*(F^{-1}) \end{aligned}\right\} \Rightarrow v(\alpha) = v^*(F^{-1})$$

and the last equality gives us explicitly the ideal belonging to $v(\alpha)$, hence

$$\delta(M) = \mathrm{cl}\,(F^{-1})$$

On the other hand we have:

$$\mathrm{cl}(M) = \mathrm{cl}(F \cdot \alpha_o) = \mathrm{cl}(F) \cdot \mathrm{cl}(\alpha_o) = \mathrm{cl}(F)$$

which shows that δ is the class map cl followed by the involution $j: x \to x^{-1}$:

$$\delta = j \circ cl.$$

We aim now at a description of the image of $U(o)$ under δ which we shall denote by im δ. We consider part of (11.6):

$$1 \longrightarrow U \longrightarrow V \xrightarrow{\beta} U(o) \xrightarrow{\delta} \mathfrak{C}(o)$$

The homomorphism $\beta: w \longmapsto w \cdot o$, $w \in V$, maps V onto the principal unit radical modules which we shall denote by $\mathfrak{B}(o)$. This observation allows us to modify the above sequence:

$$1 \longrightarrow \mathfrak{B}(o) \longrightarrow U(o) \xrightarrow{\delta} \mathfrak{C}(o)$$

From its exactness we deduce

$$U(o)/\mathfrak{B}(o) \cong \text{im}(\delta).$$

We can characterize im(δ) otherwise. The exactness of (11.6) implies that

$$1 \longrightarrow \text{im } \delta \longrightarrow \mathfrak{C}(o) \xrightarrow{\gamma} \mathbb{Q} \otimes \mathfrak{C}(o)$$

is exact, i.e. im(δ) = kern γ. kern γ in turn under the present assumption, is the torsion part of $\mathfrak{C}(o)$ (cf [7] VII, Prop.7.1) so that we obtain

$$\text{im } (\delta) = \text{Tor } \mathfrak{C}(o).$$

Together with the above remark we have shown

$$\text{Tor } \mathfrak{C}(o) \cong U(o)/\mathfrak{B}(o)$$

Considering how little information one can get on the ideal class group in general this characterization of its

torsion part by unit radical modules appears to be very welcome.

We summarize our deliberations in

(11.7) Proposition: The connecting homomorphism δ of (11.6) has the properties:

(I) $\delta = j \bullet cl$ with: $\begin{cases} cl \text{ the class map restricted to } \mathfrak{U}(o) \\ j \text{ the involution } x \to x^{-1} \end{cases}$

(II) $o \to \mathfrak{B}(o) \to \mathfrak{U}(o) \xrightarrow{\delta} \operatorname{Tor} \mathfrak{C}(o) \to o$ is exact.

(11.8) Corollary: If the underlying field K is an algebraic number field then δ has the properties:

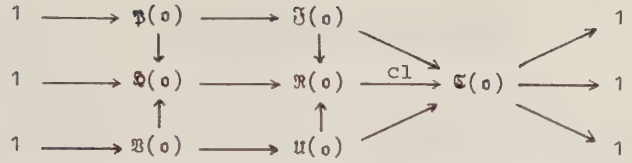
(I) δ is surjective

(II) $o \to \mathfrak{B}(o) \to \mathfrak{U}(o) \to \mathfrak{C}(o) \to o$ is exact.

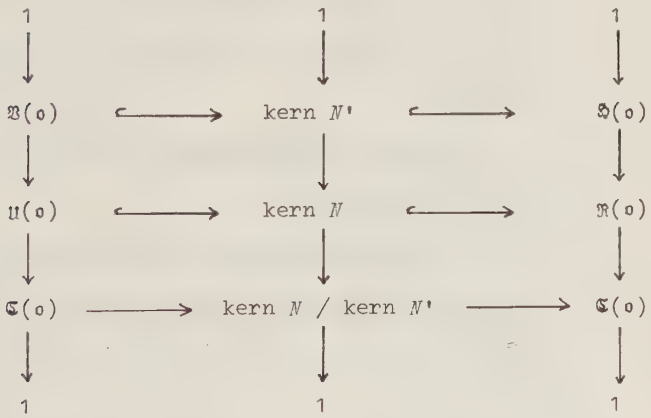
Proof: For algebraic number fields we have $\operatorname{Tor} \mathfrak{C}(o) = \mathfrak{C}(o)$ which implies the assertions.

In this case the ideal class group can be represented in terms of unit radical modules only which has no analogue in purely ideal-theoretic terms as o is the only unit in $\mathfrak{J}(o)$ and this is principal.

Thus in the case of algebraic number fields we have three exact sequences involving the ideal class group $\mathfrak{C}(o)$:



In view of this diagram one may for algebraic number fields raise the following norm problem. The kernel of N, the norm of radical modules, contains $\mathfrak{U}(o)$. The restriction N of N' to principal radical modules has a kernel containing $\mathfrak{B}(o)$. Therefore we have a diagram with exact columns:



The question now is to determine kern N/ kern N' and one might conjecture that it is not too far from the ideal class group $\mathfrak{C}(o)$.

12. An Estimate for Element - Resolvents over a $\mathfrak{p}$-adic Number Field

We turn now to a problem which is loosely connected with radicals. We are going to consider special radicals over a $\mathfrak{p}$-adic number field which arise as element-resolvents and which were described in a paper of Fröhlich's ([2]). We take the opportunity to answer a question which was raised there.

We start off from the following situation:

K a $\mathfrak{p}$-adic number field, not necessarily complete but containing those roots of unity which will be needed (namely all n-th roots of unity with $n / |\Gamma|$, Γ a Galois group which will be defined presently).

$A \supset K$ is a finite separable normal extension of K with Galois group Γ.

φ: $A \to \mathbb{P}$ a discrete valuation of A; φ shall be normalized such that it will induce on $\mathbb{Q} \subset A$ the usual p-adic valuation, $(p) = \mathfrak{p} \cap \mathbb{Z}$, i.e. $\varphi(p) = p^{-1}$.

Every matrix-representaion of Γ over K of degree n gives rise to a character $\chi: \Gamma \to K$.

For each character χ of degree n there is a form Φ_n of A in $R(A/K) \cup o$ defined by the element-resolvent (a/χ) (cf.[2], Theorem 3.1; 3.4)

$$\Phi_n: \quad a \longmapsto (a/\chi)$$

This form in turn can be characterized as the irreducible factor Φ_n of Frobenius' group determinant belonging to the character χ of degree n. (cf.[2]).

Using Frobenius' explicit formula ([3], § 3 (8)) for this form we can link the value of an element $a \in A$ to that of the radical (a/χ), its resolvent.

(12.1) Theorem:

$$\varphi(a/\chi) \leq \frac{\varphi(a)^n}{\varphi(n!)}, \quad n \text{ the degree of } \chi$$

Proof: Frobenius' formula runs as follows:

$$\Phi_n(x) = \sum \frac{(-1)^{a_1+a_2+\ldots+a_n} s_1^{a_1} \cdot s_2^{a_2} \ldots s_n^{a_n}}{1^{a_1} \cdot 2^{a_2} \ldots n^{a_n} \cdot a_1! a_2! \ldots a_n!}$$

the sum being extended over all n-tuples $a_1, a_2, \ldots, a_n$ with the property:

$$a_1 + 2a_2 + \ldots + na_n = n \text{ and } a_i \geq 0 \text{ integer.}$$

The S_k, $k = 1,2,\ldots,n$, are symmetric functions with sums of roots of unity as coefficients:

$$S_k = \sum_{\gamma_1, \gamma_2 \ldots \gamma_k \in \Gamma} \chi(\gamma_1, \gamma_2, \ldots \gamma_k) \cdot x_{\gamma_1} x_{\gamma_2} \ldots x_{\gamma_k}$$

In our interpretation we have to identify:

$$(a/\chi) = \Phi_n(a)$$

$$x_{\gamma_i} = a_{\gamma_i} \quad \text{with } a \in A, \gamma_i \in \Gamma, \; i = 1,2,\ldots,n$$

The operation of the γ on a written from the right.

By the properties of the discrete valuation φ we get:

$$\varphi(a/\chi) \leq \max_{\Sigma ka_k = n} \left[\frac{\varphi(s_1^{a_1} \cdot s_2^{a_2} \cdots s_n^{a_n})}{\varphi(1^{a_1} 2^{a_2} \cdots n^{a_n} a_1! \cdots a_n!)} \right]$$

To obtain a bound we have to determine the maximum of the numerator and the minimum of the denominator.

1) For the S_k we get:

$$\varphi(S_k) \leq \max_{\gamma_1, \ldots \gamma_k \in \Gamma} \left\{ \varphi\left(\chi(\gamma_1, \gamma_2, \ldots, \gamma_k) \cdot a\gamma_1 \cdot a\gamma_2 \cdots a\gamma_k \right) \right\}$$

$$= \max \left\{ \varphi(\chi(\gamma_1, \gamma_2, \ldots, \gamma_k)) \cdot \varphi(a\gamma_1 \cdot a\gamma_2 \cdots a\gamma_k) \right\}$$

We note that $\varphi(a) = \varphi(a\gamma)$ for all $\gamma \in \Gamma$ and get:

$$\varphi(S_k) \leq \varphi(a)^k \cdot \max \varphi(\chi(\gamma_1, \gamma_2, \ldots, \gamma_k)$$

$\chi(\gamma_1, \gamma_2, \ldots, \gamma_k)$ being a sum of n-th roots of unity we have $\varphi(\chi(\gamma_1, \gamma_2, \ldots, \gamma_k)) \leq 1$ for all possible arguments of χ, so:

(12.2) $\varphi(S_k) \leq \varphi(a)^k$.

We need a statement on $\prod_{i=1}^{n} s_i^{a_i}$:

$$\varphi(s_1^{a_1} \cdot s_2^{a_2} \cdots s_n^{a_n}) = \varphi(s_1)^{a_1} \cdots \varphi(s_n)^{a_n}$$

$$\leq \varphi(a)^{1 \cdot a_1} \cdot \varphi(a)^{2 \cdot a_2} \cdots \varphi(a)^{n a_n} = \varphi(a)^n$$

Therefore, independently of the individual a_i,

$$\varphi(s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n}) \leq \varphi(a)^n$$

and

$$\max_{\Sigma a_k k = n} \varphi(s_1^{a_1} s_2^{a_2} \cdots s_n^{a_n}) \leq \varphi(a)^n.$$

2) Set $c = 1^{a_1} 2^{a_2} \ldots n^{a_n} \cdot a_1!\, a_2! \ldots a_n!$

For given a_i, $i = 1,2,\ldots,n$, the denominator in question, $\varphi(c)$, can easely be determined. But in our case a difficulty arises from the indirect way the a_i are prescribed. We must consider all n-tuples of integers satisfying

$$a_1+2a_2+\ldots + na_n = n.$$

It is more convenient here to work with an exponential valuation w and we choose to go over to $w(m) = -\log \varphi(m)$ ($w(0) = \infty$). Then the minimum of the $\varphi(c)$ will correspond to the maximum of the $w(c)$ which we will determine now.

$$w(c) = w\Big(\prod_{\nu=1}^{n} a_\nu!\, \nu^{a_\nu}\Big) = \sum_{\nu=1}^{n} w(a_\nu!\, \nu^{a_\nu})$$

To evaluate this sum we use the following facts which will be proved in the sequel:

$$(1)\quad w\,(m^a\, a!) \leq w((ma)!) \qquad a, m \in \mathbb{N}$$

$$(2)\quad w\Big(\Big(\sum_{i=1}^{n} k_i\Big)!\Big) \geq \sum_{i=1}^{n} w(k_i!),\ k_i \in \mathbb{N}$$

Therefore:

$$w(c) \leq \sum_{\nu=1}^{n} w((\nu a_\nu)!) \leq w((\textstyle\sum \nu a_\nu)!) = w(n!)$$

or in terms of the valuation φ:

$$(12.3)\qquad \varphi(c) \geq \varphi(n!)$$

independently of the individual a_i. Both estimates together yield the statement of the theorem.

We are left with the proofs of the following

(12.4) Lemma: Let a,m,k_i ($i \in \mathbb{N}$) be natural numbers and w an exponential valuation of $\mathbb{Q}$. Then:

(1) $m^a\, a! \leq (ma)!$

and $w(m^a\, a!) \leq w((ma)!)$

(2) $k = \sum_{i=1}^{l} k_i$ implies

$k! \geq k_1!\, k_2! \ldots k_l!$

$w(k!) \geq w(k_1!) + w(k_2!) + \ldots + w(k_l!)$

Proof: To see (1) we arrange the factors of (ma)! in a rectangular fashion:

1	2	...	m-1
m	m+1	...	2m-1
2m	2m+1	...	3m-1
(a-1)m	(a-1)m+1	...	am-1
am			

The product of the numbers of the first column is exactly $m^a \cdot a!$ Therefore

$(ma)! = m^a a! \cdot A$ with an integral A

which yields both assertions (1):

$(ma)! \geq m^a a!$

$w(ma)! = w(m^a a!) + w(A),\ w(A) \geq 0$

$w(ma)! \geq w(m^a a!)$ q.e.d.

The second part needs a little more care. We are giving independent proofs of the global and local parts of the

assertion. Firstly we show $k! > k_1!k_2!\ldots k_l!$ by induction.

$l = 1 \quad k = k_1 \quad \Rightarrow \quad k! = k_1!$

$l = 2 \quad k = k_1+k_2;\ k_1, k_2 \neq o$

$$k! = k_1!\,(k_1+1)(k_1+2)\ldots(k_1+k_2)$$

$$= k_1! \cdot \sum_{\nu=o}^{k_2} k_1^{\nu}\, s_\nu$$

where the s_ν are the elementary symmetric functions in $1,2,3,\ldots,k_2$, especially $s_o = k_2!$

Therefore:

$$k! > k_1!\, s_o = k_1!k_2! \text{ for } k_2 > o$$

We now assume that the assertion holds for all $i < l$.
Let $k = \sum_{i=1}^{l} k_i = (k_1+k_2+\ldots+k_{l-1})+k_l$.

Then (cf $l=2$):

$$\left.\begin{array}{l} k! \geq (k_1+k_2+\ldots+k_{l-1})!\, k_l! \\ \text{assumption: } (k_1+\ldots+k_{l-1})! \geq k_1!\ldots k_{l-1}! \end{array}\right\} \Rightarrow k! > \prod_{i=1}^{l} k_i!$$

which was to be proved.

Secondly we turn to $w(k!) \geq w(k_1!)+w(k_2!)+\ldots+w(k_l!)$ and again apply induction on the number l of summands. It is appropriate here to go over to the p-adic representation of these summands with respect to the residue system $o,1,2,\ldots,p-1$. For an integer $k = \sum_i \varkappa_i p^i$ we then have at our disposal Hensel's formula for $w(k!)$:

$$w(k!) = \frac{k-q}{p-1}, \quad q = \sum_i \varkappa_i$$

a) For two summands (l=2) we have to show:

$k = r+s \Rightarrow w(k!) \geq w(r!)+w(s!)$

Let $r = \Sigma\, r_i p^i$, $s = \Sigma\, s_i p^i$, $o \leq r_i, s_i < p$

denote the p-adic representations of r and s. Then, by Hensel's formula, we get:

$$\left.\begin{aligned}(p-1)\ w(r!) &= r - \Sigma\, r_i \\ (p-1)\ w(s!) &= s - \Sigma\, s_i\end{aligned}\right\} \Rightarrow (p-1)[w(r!)+w(s!)] = k-\Sigma(r_i+s_i)$$

The problem accordingly reduces to

$$w(k!) \geq w(r!)+w(s!) \quad \Leftrightarrow \quad \Sigma\, \varkappa_i \leq \Sigma(r_i+s_i).$$

At this stage we make the following general observation: The addition of two p-adic numbers represented with respect to the residue system o,1,2,...,p-1 produces at each place at most 1 as carry. To see this consider:

$$\Sigma\, a_i p^i + \Sigma\, b_i p^i = \Sigma\, c_i p^i,\ o \leq a_i, b_i, c_i < p$$

and distinguish two cases:

(1) $a_i+b_i \leq 2p-2$ i.e. $a_i+b_i = c_i+\nu p$; ν=o,1

(2) $a_j+b_j+1 \leq 2p-1$ i.e. $a_j+b_j+1 = c_j+\nu p$; ν =o,1

where (2) represents the case in which a carry from the preceding place has to be regarded. This has the property that the sum a_j+b_j+1 from which c_j is being computed does not exceed 2p-1, so that in turn it produces at most 1·p as carry.

Applying this observation to the situation k = r+s we get two cases:

(1) $\varkappa_i = r_i+s_i - \delta p$ with $\delta = 0$ or 1

or (2) $\varkappa_i = r_i+s_i+1 - \delta p$

In the first case $\varkappa_i \leqq r_i+s_i$ will hold. If the second case occurs we only get

$$\varkappa_i \leqq r_i+s_i+1$$

But then certainly for the preceding $\varkappa_{i-1}$ we must have

$$\varkappa_{i-1} = r_{i-1}+s_{i-1} -(p-\delta)$$

$$\varkappa_{i-1} \leqq r_{i-1}+s_{i-1} - 1 \text{ as } p \geqq 2,$$

and adding both

$$\varkappa_{i-1}+\varkappa_i \leqq (r_{i-1}+r_i) + (s_{i-1}+s_i)$$

So we may conclude for the sum

$$\Sigma\ \varkappa_i \leqq \Sigma\ r_i + \Sigma\ s_i$$

which we have already seen to be equivalent to our assertion.

b) It is easy now to complete the induction. Assuming the assertion holds for all $i < l$ write $\sum_{i=1}^{l} k_i = (k_1+k_2+\ldots+k_{l-1})+ k_l = k$. Then:

$$\left.\begin{array}{l} w(k!) \geqq w\left[\left(\sum_{i=1}^{l-1} k_i\right)!\right] + w(k_l!) \text{ (by a) } \\ w\left[\left(\sum_{i=1}^{l-1} k_i\right)!\right] \geqq \sum_{i=1}^{l-1} w(k_i!) \text{ by assumption} \end{array}\right\} \Rightarrow$$

$$\Rightarrow w(k!) \geqq w(k_1!) + w(k_2!) + \ldots + w(k_l!) \quad \text{q.e.d.}$$

L I T E R A T U R E

Papers:

[1] A. Fröhlich: Radical Modules over a Dedekind Domain

Nagoya Math. Journ. 27(1966) p. 643 - 662

[2] A. Fröhlich: Resolvents, Discriminants, and Trace Invariants

Journal of Algebra 4 (1966) p. 173 - 198

[3] G. Frobenius: Über die Primfaktoren der Gruppendeterminante

Sitzungsber. d. Akad. Berlin, 1896 p. 1343 - 1382

[4] A. Kertesz: Systems of Equations over Modules

Acta Sci. Math. Szeged 18(1957) p. 207 - 234

[5] H. Minkowski: Über die positiven quadratischen Formen und über kettenbruchähnliche Algorithmen

Journ. für Reine und Angew. Math. 107(1891), p. 278 - 297

[6] H. Minkowski: Geometrie der Zahlen

Leipzig 1896, § 40.

Textbooks:

[7] Cartan-Eilenberg: Homological Algebra
Princeton 1956

[8] Cassels-Fröhlich: Algebraic Number Theory
London-New York 1967

[9] Dirichlet-Dedekind: Vorlesungen über Zahlentheorie(Supplement XI)
4^{th} edition, Braunschweig 1894

[10] H. Hasse: Zahlentheorie
2^{nd} edition, Berlin 1963

[11] K. Hensel: Zahlentheorie
Berlin-Leipzig 1913

[12] A. Kertesz: Vorlesungen über Artinsche Ringe
Leipzig 1968

Symposia:

[13] U. Güntzer: Transitivity Theorems for the Non-Archimedean Spectral Semi-Norm of Ring Extensions

The Greek Mathematical Society
C. Caratheodory Symposium 1973 p.173-195

V I T A

Am 12. Mai 1933 wurde ich in Plauen im Vogtland geboren als Sohn des medizinischen Fachkaufmanns Andreas Wicke und seiner Ehefrau Rosa geb. Traut.

Nach dem Besuch der heimatlichen Grundschule (1939-1943) und des sprachlichen Zweiges der Staatlichen Oberschule für Jungen (1943-1951) legte ich 1951 das Abitur ab und erlangte meine weitere Ausbildung in Mathematik, Astronomie und Physik an den Universitäten Jena (1952-1957), FU Berlin (1958-1960) und Queen Mary College, London (1961-1962). - In Jena besuchte ich vor allem Vorlesungen der Professoren Brödel, Maier,Lambrecht, Hoppe, Buchwald, Schuster; in Berlin Ostmann, Grotemeyer, Dinghas, Hinderer, Ludwig; in London Hirsch, Fröhlich, Gruenberg.

In Berlin erlangte ich im Jahre 1960 das Diplom der Mathematisch Naturwissenschaftlichen Fakultät der FU mit einer Arbeit über p-adische Zahlen und Wittsche Vektoren. 1963 lehrte ich im Rahmen einer Tutorial Studentship am King's College der Universität London. Seit 1965 bin ich als wissenschaftlicher Assistent am II. Mathematischen Institut der Freien Universität tätig.

Allen meinen akademischen Lehrern danke ich für Förderung und Anregung, insbesondere Herrn Professor Fröhlich, London, auf dessen Untersuchungen die vorliegende Arbeit zurückgeht und der mich bei der Abfassung dieser Arbeit bereitwilligst unterstützte.